VVB magazin

2/2022
Erscheint 6 x im Jahr
Einzelheft € 5,-
57. Jahrgang
15. April 2022

Sonderausgabe für Networker Solutions

Hybrid-Tagung des Fachkreises BO/IT zum Thema

Top-Risiko Cyber und Strategien

Seiten 28-43

MV 2022 HANNOVER
20./21. MAI 2022
Programm der Fachtagung
Partnerprogramm

Treffpunkt Mannheim
Online-Veranstaltung zum Lieferkettengesetz

ivwKöln
eine ganz „persönliche" Beschreibung des Instituts

DVfVW
Ein studentischer Blick auf die Jahrestagung des DVfVW

Liebe Mitglieder, Förderer und Freunde unserer VVB,

am Sonntag, 20. März, war der kalendarische Frühlingsanfang. Was sagt uns das? Nun, mindestens zwei Dinge: Erstens können wir auf besseres Wetter hoffen. Einige Tage mit viel Sonnenschein und angenehm milden Temperaturen wurden uns schon beschert. Die Natur blüht auf und lässt allmählich ihre Farbenpracht wieder erkennen, was nicht zuletzt auch unserer Stimmung und unserer Gesundheit zugutekommt – mal abgesehen von den unerwünschten Nebeneffekten eines allzu argen Pollenflugs für die Allergiker unter uns. Zum anderen bedeutet der Frühling für die VVB, dass die Mitgliederversammlung (MV) bevorsteht. Am 20. und 21. Mai 2022 ist es so weit und wir dürfen wieder einmal zu Gast in Niedersachsens Landeshauptstadt Hannover sein, auch dank des Sponsorings der VGH, des HDI und weiteren Förderern. Sofern Sie nicht bereits angemeldet sind, empfehle ich Ihnen, dieses zeitnah nachzuholen. Gute Gründe gibt es dafür eine ganze Menge. Da wäre etwa das Treffen mit guten Bekannten, Freunden und beruflich verbundenen Menschen – das Gesellschaftliche und das Networking. Ob beim Kommersabend, beim Partnerprogramm, der eigentlichen MV oder den Fachkreisveranstaltungen. Oder, um Letzteres aufzugreifen, das Fachliche. Denn auch dieses Mal wird es wieder diverse thematische „Leckerbissen" geben, um auf gewohnt hohem Niveau Vorträge zu erleben und fachliche Austausche zu führen. Und als drittes Beispiel sei die Vorstandswahl der VVB erwähnt. Mischen und gestalten Sie mit, liebe Mitglieder unserer Vereinigung, und machen von Ihrem Stimmrecht Gebrauch. Neben der Briefwahl haben Sie auf der MV in Hannover letztmalig für diese Periode die Chance, Ihr Votum abzugeben. Alle, die kandidieren, danken Ihnen für Ihr Feedback und eine hohe Wahlbeteiligung, mich selbstverständlich eingeschlossen. Die Ergebnisse werden dann wie üblich live bekannt gegeben. Sofern also Corona uns auf der Zielgeraden keinen Strich durch die Rechnung macht, freue ich mich schon jetzt ganz besonders auf ein möglichst zahlreiches Wiedersehen „in persona" mit Ihnen!

Im vorangegangenen VVBmagazin 1/2022 haben wir Ihnen die Tagung „Toprisiko Cyber" des Fachkreises BO/IT angekündigt. Diese fand Mitte März statt und darf als voller Erfolg bezeichnet werden. In dieser Ausgabe, meine sehr verehrten Leserinnen und Leser, präsentieren wir Ihnen die umfangreiche Berichterstattung zu diesem hochkarätigen Event mit der Referentin Silvana Rößler und den Referenten Dr. Matthias Orthwein, und Nicolai Wojciechowski.

Darüber hinaus finden Sie bei den Treffpunkten neben lohnenswerten Termin-Notizen auch die Abhandlung von Stephan Best, dem neuen Treffpunktleiter Mannheim, welcher über eine spannende Veranstaltung zum Thema „Lieferkettengesetz" schreibt.

Weiterhin können Sie im Inneren dieses Heftes einiges aus dem ivwKöln entdecken, die Einladung zum fast schon legendären Golf-Turnier, das die VVB seit vielen Jahren begleitet, sowie den aus studentischer Sicht verfassten Bericht über die Jahrestagung des DVfVW.

Genießen Sie mit alldem und den weiteren Inhalten wie immer das Studium des VVBmagazin und bleiben Sie uns gewogen.

Und: Passen Sie gut auf sich auf und bleiben Sie gesund!

Ihr

Stefan van Marwyk

INHALT

Top-Risiko Cyber und Strategien

Bericht von der Veranstaltung des Fachkreises BO/IT am 16. März 2022

von REINHOLD FALLER (F/B) und BERND SEBALD (kor. M.)

Seit einigen Jahren halten wir bereits den Kontakt zum BWV in München, vor allem über die DVA, und haben seit langem schon vereinbart, dass wir einmal eine gemeinsame Veranstaltung durchführen wollen. Als letztes Jahr im Herbst der bisherige Geschäftsführer des BWV, Herbert Schmidt, seinen Abschied nahm (s. Reinholds Bericht über die Verabschiedung im Magazin 06/2021), wurde das Angebot zu einer gemeinsamen Veranstaltung vom BWV erneuert, in deren Räumlichkeiten zu tagen. Gemeinsam brüteten wir mit seinem Nachfolger Lars Moormann über Themen und machten dann Nägel mit Köpfen. Einige Zoom-Sessions mit Lars… dann standen Thema und Datum fest.

Hanno Pingsmann

Michael Steimer

Am 16. März 2022 war es endlich soweit, die erste Veranstaltung in hybrider Form wurde vom Fachkreis BO/IT in Kooperation mit dem BWV München und tatkräftiger Unterstützung durch unser VVB-Mitglied Michael Steimer (Cyber-Experte und Fachkreisleitung Cyber) organisiert. Dabei wurde die Veranstaltung bewusst in zwei Teile aufgeteilt. Der erste Teil am Nachmittag von 14:00 – 17:00 Uhr war für die Praktiker gedacht und der zweite Teil von 17:30 – 19:30 Uhr wurde der Cyber-Strategie gewidmet. Im ersten Teil referierten 3 Experten und beantworteten im Anschluss Fragen. Im Zweiten Teil kamen zunächst 2 Impulsvorträge und im Anschluss moderierte unser VVB-Mitglied Patrick Hamann eine erweiterte Diskussionsrunde. Dazwischen führten wir von unserem Fachkreis BO/IT die angekündigte Beiratswahl durch.

Zu Beginn des 1. Teils stellte der neue Geschäftsführer des BWV München, Lars Moormann, das BWV München kurz vor. Anschließend folgte durch Reinhold der Werbetrailer der VVB.

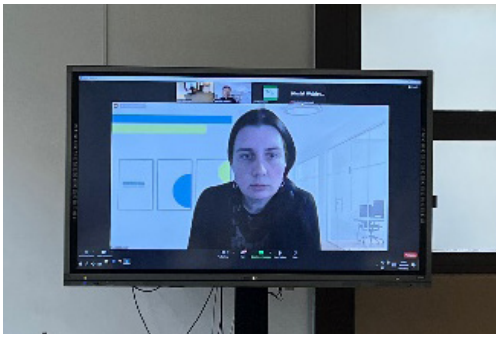
Im Anschluss stimmte Michael Steimer die Teilnehmer auf die nachfolgenden Referenten ein und machte dabei deutlich, wie wichtig heute eine Cyberabdeckung für Unternehmen ist.

Als erster Referent stellte Hanno Pingsmann, der Gründer und Geschäftsführer der CyberDirekt GmbH in Berlin, seine Studie vor. In der Studie wurde unter anderem untersucht, wie gut kleine und mittlere Unternehmen (KMU) in Deutschland im Bereich Cyber abgesichert sind. Ein großer Teil dieser Unternehmen war bislang nicht von Cyber-Angriffen betroffen. Das kann ein gefährliches Wiegen in falsch gefühlter Sicherheit sein. Allerdings spricht auch niemand in der Öffentlichkeit darüber, ob sein Unternehmen gehackt wurde. Als größte Gefahrenquellen werden schwache Passwörter und die Nutzung öffentlicher WLAN-Netzwerke genannt. Um den Gefahren zu begegnen, nutzen Firmen hauptsächlich Virenschutz, Firewall, starke Passwörter, VPN-Verschlüsselung und regelmäßige Passwortänderungen als Basissicherung. Beim Einspielen von Sicherheitsupdates (Patch-Management) „ist noch viel Luft nach oben“ und das ist oft ein Einfallstor für Hacker. Bedingt durch Corona hat sich der Anteil an Homeoffice bekanntermaßen sehr gesteigert, nur in 15,7 % der Unternehmen wurde ausschließlich in Präsens gearbeitet. Durch den daraus resultierenden erhöhten Homeoffice-Anteil wurde ein weiteres großes Einfallstor für Hacker geöffnet, sofern dafür keine Sicherheitsmaßnahmen ergriffen wurden. Ein weiterer Sicherheitsfaktor sind die Mitarbeiter/innen, die regelmäßig in IT-Sicherheit geschult werden müssen. Hier gibt knapp ein Fünftel der befragten Unternehmen an, die eigenen Mitarbeitenden nicht regelmäßig zu schulen.

Als weiteres Ergebnis der Umfrage in der Studie kam unter anderem heraus, dass nur 23 % der Unternehmen über eine Cyberabsicherung verfügen und 18 % der Unternehmen noch einen passenden Schutz suchen. 59 % der Unternehmen haben sich damit noch nicht befasst oder erachten diese Absicherung nicht für notwendig. Für die Versicherungswirtschaft ist hier noch hohes Abschlusspotential vorhanden. Hanno Pingsmann gab uns zum Ende seines Vortrags noch einen Ausblick, wonach

die Cybersparte die am stärksten wachsende Versicherungsparte bleibt, die Anforderungen an IT-Sicherheit werden weiter steigen, und nicht jedes Unternehmen wird eine Cyber-Versicherung bekommen.

Wie wichtig eine Cyberabdeckung ist, stellte uns unser neues VVB-Mitglied Silvana Rößler (Head Security Response bei der Networker solutions GmbH) in Ihrem spannenden Vortrag vor, in dem Sie recht lebhaft aus ihrer Praxis berichtete. Lesen Sie dazu den Fachbericht, den uns Silvana in diesem VVB-Magazin beigesteuert hat. Besonderheit am Rande: Sie ist künftig auch im Auftrag der TH Köln bei Prof. Michael Fortmann Dozentin für den Zertifikatslehrgang „Cyber Insurance Manager*in".



Silvana Rößler

Zum Ende des erstens Teils referierte das zweite neue VVB-Mitglied Dr. Matthias Orthwein (Partner SKW Schwarz Rechtsanwälte) über das Thema „Alles was (Cyber)Recht ist." mit Schwerpunkt DSGVO. Wer gedacht hatte, hier kommt ein trockener juristischer Vortrag, der irrte sich gewaltig. Lesen Sie dazu den Fachbeitrag, den Dr. Matthias Orthwein in diesem VVB-Magazin für uns geschrieben hat.

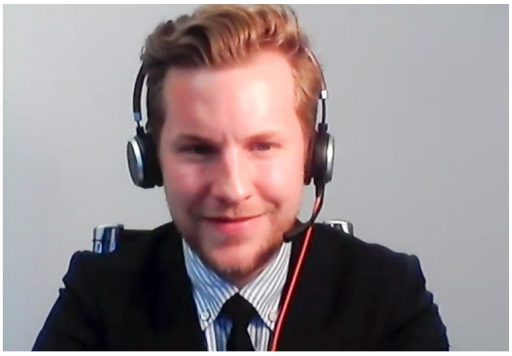
Nach dem Vortrag von Dr. Orthwein lud das BWV die anwesenden Gäste zu einem Imbiss ein. In der Zwischenzeit führte der Fachkreis BO/IT seine Beiratswahl virtuell durch.

Pünktlich um 17:30 Uhr begannen wir mit dem 2. Teil, der „Cyber Strategie". Den Anfang machte Matthias Daum (Senior Underwriter Cyber bei AGCS CEE) mit einem Impulsvortrag zum Cyber-Management 2022. Danach ist Cyber eine Management-Herausforderung im Spannungsfeld der Mitarbeiter, Kunden, Schäden und dem Umfeld. So sind bei den Mitarbeitern die Soft Skills immer entscheidender. Auf der einen Seite erfordert Cyber von den Mitarbeitern ein breites fachliches Spektrum und muss den Mitarbeitern Spaß machen. Auf der anderen Seite haben die Kunden einen hohen Bedarf nach Cyberabsicherung, wobei die Sicherheit oft unzureichend ist. So müssen Kunden über den Gesamtprozesse begleitet werden. Gleichzeitig gibt es im Umfeld enorme Veränderungen durch Gesetzgebung, Angreifer und zunehmende Sicherheitslücken. Schadenhöhe und Frequenz nehmen zu, wobei 80% der Schäden einfach vermeidbar wären, zum Beispiel durch ein gutes Patchmanagement. Unter den Geschäftsrisiken in Deutschland nehmen Cybervorfälle mit 50% nach der Betriebsunterbrechung mit 55 % den 2. Platz ein. Insofern zeigt das auch hier wieder, wie wichtig eine Absicherung gegen Cyberrisiken ist.

Dr. Matthias Orthwein

Matthias Daum

Im zweiten Impulsvortrag berichtete unser drittes neues VVB-Mitglied Nicolai Wojciechowski (Rechtsanwalt bei BLD Bach Langheid Dallmayr) mit seinem Vortrag zu „Obliegenheiten und Ausschlüsse – Aktuelle Herausforderungen bei der Versicherbarkeit von Cyberrisiken", wie er Cyber in seiner Tätigkeit als Anwalt erlebt. Lesen Sie dazu seinen eigenen Fachbericht in diesem VVBmagazin.



VVB-Mitglieder: links Patrick Hamacher/rechts Nicolai Wojciechowski

Nach diesen beiden Impulsvorträgen übernahm unser VVB-Mitglied Patrick Hamacher (der Makler mit der Cap, vielen bekannt vom Podcast „Versicherungsgeflüster“) die Moderation der anschließenden Podiumsdiskussion zwischen Hanno Pingsmann, Michael Daum, Dr. Matthias Orthwein und RA Nicolai Wojciechowski. Hier ging es um das Thema „Quo vadis Cyberversicherung“. Das Thema ist brandaktuell, da von einigen Versicherern in Frage gestellt wird, ob man Cyberrisiken in Zukunft noch absichern kann. So gab es zwei Tage vor unserer Veranstaltung einen Pressebericht der Munich Re, in dem diese bekannt gab, sich aus dem Cyber-Geschäft zurückziehen zu wollen. Nebenher streute Patrick Hamacher noch zusätzlich die Fragen der Teilnehmer ein, die im Chat gestellt und damit gleich beantwortet werden konnten.

Um 19:30 Uhr beendete unser Moderator Patrick Hamacher pünktlich die Diskussionsrunde, die noch deutlich länger hätte dauern können. Reinhold und unser Gastgeber Lars Moormann verabschiedeten sich zum Ausklang bei den anwesenden Teilnehmern, den virtuellen Zuhörern und bedankten sich bei den Referenten.

Rundum war es eine sehr gelungene Veranstaltung. Wir hatten über 143 Anmeldungen aus dem Teilnehmerkreis der VVB, dem BWV München und dem VGA München.

In diesem Zusammenhang möchten wir noch auf ein absolutes Highlight hinweisen: Infolge unserer Gespräche mit Lars Moormann vom BWV wird das BWV zusammen mit Michael Steimer (aus der Fachkreisleitung Cyber) eine 5-tägige Ausbildung zum „Experte/-in Cyberversicherung (BWV) anbieten. Weitere Informationen dazu finden Sie unter https://muenchen.bwv.de

Abschließend möchten wir uns im Besonderen bei Lars Moormann und Michael Steimer bedanken. Ohne diese beiden wäre das in der Form nicht möglich gewesen. Michael mit seiner Expertise als Cyber-Spezialist und Lars, der uns grosszügig mit seiner Organisation und der Infrastruktur des BWV ein hoch professionelles Umfeld zur Verfügung gestellt hat. Wir waren uns einig, dass dies ein gelungener Auftakt war, der Fachkreis BO/IT und das BWV werden das fortführen. Es war ein voller Erfolg, das beweist auch das Ergebnis einer Umfrage des BWV über diese Veranstaltung. Hier vergaben die Teilnehmer im Durchschnitt 4,8 von möglichen 5 Sternen. Freuen Sie sich schon jetzt, es werden weitere Veranstaltungen in Kooperation mit dem BWV München folgen.

Von links die Akteure in Präsenz: Lars Moormann, Hanno Pingsmann, Michael Daum, Dr. Matthias Orthwein, Reinhold Faller

Silvana Rößler ist Diplom-Informatikerin mit einem Master in digitaler Forensik. Sie verfügt über 10 Jahre Erfahrung im Bereich digitale Forensik und Informationssicherheit und leitet den Bereich Security Incident Response bei der networker, solutions GmbH. Hierbei verantwortet sie auch die Durchführung einer Vielzahl von Projekten und forensischen Untersuchungen im Rahmen der Security Incident Response zur Aufklärung und Mitigierung von Informationssicherheitsvorfällen. Neben ihren Aufgaben als Führungskraft und IT-Forensikerin hält sie Vorträge, Seminare und Schulungen und arbeitet an Veröffentlichungen von Fachbeiträgen.

Die unterschätzte Schwachstelle im System

Der Faktor „Mensch“

von SILVANA RÖßLER (kor. M.)

„Wie konnte uns so etwas passieren?“ Unternehmen, welche diese Frage stellen, haben etwas gemeinsam. Egal, ob es sich um einen kleinen Betrieb, um ein mittelständisches Unternehmen oder um einen international agierenden Konzern handelt – sie wurden Opfer eines Cyberangriffs.

Es ist die Frage nach dem Einfallstor, nach dem berühmten Patienten Null, die Frage, wann und wie Unbefugte unbemerkt die Systeme kompromittieren konnten. Doch wie kann es so weit kommen, dass Unternehmen Opfer von Cyber-Kriminellen werden?

Neben Schwachstellen, Sicherheitslücken und Fehlkonfigurationen in Software- und Hardwarekomponenten gibt es nach wie vor ein weiteres wichtiges und attraktives Einfallstor für Cyber-Kriminelle: den Faktor „Mensch".

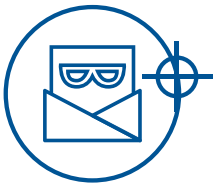
Der Mensch, aus dem Bauch entscheidend, unvorsichtig oder auch nur müde, unter Zeitdruck, mit Unsicherheit, Angst oder getrieben von Geld und Ruhm. Diese Eigenschaften und Situationen machen sich Cyber-Kriminelle zu nutze. Mithilfe mehr oder weniger ausgefeilter Techniken des Social-Engineerings versuchen diese, ihre Opfer zu der gewünschten Handlung zu bewegen. Dabei kann es sich um die Herausgabe von sensiblen Informationen wie Zugangsdaten handeln. Aber auch Kontoinformationen sind bei Cyber-Kriminellen ein beliebtes Gut. Hierzu gehören die vermeintlichen Anrufe des Microsoft-Kundendienstes. Was anfangs wie ein guter Service klingt, ist in Wahrheit eine groß angelegte Betrugsmasche.

DER FALSCHE MICROSOFT-SUPPORT

Opfer dieser Betrugsmasche berichten unter anderem davon, dass sich am Telefon ein „Mitarbeiter“ von Microsoft mit sehr schlechtem Deutsch meldet. Beginnt man mit diesem eine Unterhaltung, wird man durch eine geschickte Gesprächsführung in ein oftmals stundenlanges Telefonat verwickelt. Dem Opfer wird mitgeteilt, dass sein Computer von Schadcode betroffen sei. Dies könne es erkennen, wenn es auf ein bestimmtes Programm klickt. Dort wären Tausende Fehler zu sehen. Dazu lassen die Cyber-Kriminellen ihre Opfer demonstrativ Befehle eingeben oder die Ereignisanzeige öffnen. Um diese konstruierten „Fehler“ zu bereinigen, leitet man das verängstigte Opfer an, mittels Google-Suche

ein Fernwartungsprogramm herunterzuladen, zu installieren und zu starten. Nach einer Übermittlung des Zugangscodes erlangt der Kriminelle so uneingeschränkten Zugriff auf den Computer seines Opfers.

Währenddessen werden die Opfer gezielt über ihr Benutzerverhalten, Onlinebanking und zu ihren Bankdaten ausgefragt. Betroffene berichten außerdem, dass ihnen mitgeteilt wurde, dass sie sämtliche externen Datenträger (USB-Sticks, externe Festplatten etc.) zur Überprüfung an ihren Computer anschließen müssen.



Dieser fatale Fehler wird meistens erst dann realisiert, nachdem man bemerkt hat, dass sämtliche Daten auf den externen Datenträgern gelöscht wurden. Aber auch hierfür hat der Anrufer eine plausibel klingende Begründung. Die Daten seien im Hintergrund zwecks Überprüfung zu Microsoft übertragen worden. Nach der erfolgten Überprüfung werden diese wieder zurückgespielt. Es verwundert nicht, dass die versprochene Überprüfung weitere Überraschungen bereithält. So wird dem Opfer mitgeteilt, dass keine gültige „Mutterlizenz“ vorläge. Anschließend öffnet der Anrufer im Internetbrowser eine Webseite, welche zeigt, was der Erwerb dieser Mutterlizenz kosten würde. Erst nach dem Erwerb dieser könnten die Daten wieder zurückgespielt werden. Hierzu hat der Cyber-Kriminelle bereits aus den vorab erfolgten Gesprächen den Zugang zum Onlinebanking des Opfers vorbereitet. Der nächste Schritt ist dann nur noch, mit den abgegriffenen Daten sich selbst bei der Bank anzumelden, einen kurzen Blick auf die Bonität des Opfers zu werfen und eine Echtzeitüberweisung vorzubereiten. Die notwendige Aufforderung der Legitimierung erfolgt dann über die vertraute App beim Opfer, das diese gerne freigibt und den vermeintlich geringen Betrag bezahlt, um schnell wieder an seine Daten zu kommen. Das Opfer bekommt währenddessen von den im Hintergrund ausgeführten Überweisungen nichts mit, sondern wird meistens auch noch aufgefordert, weitere Überweisungsbestätigungen der App zu quittieren, um endlich in den Genuss der „Mutterlizenz“ zu gelangen.

› Die Daten seien im Hintergrund zwecks Überprüfung zu Microsoft übertragen worden. Nach der erfolgten Überprüfung werden diese wieder zurückgespielt. Es verwundert nicht, dass die versprochene Überprüfung weitere Überraschungen bereithält.

Erst nach Ende des Telefonates und einer erneuten Anmeldung des Betroffenen an seine Online-Bank wird klar, dass man doch einige tausend Euro mehr für die „Mutterlizenz“ bezahlt hat, als gedacht.

Wer solche Anrufe vom falschen Microsoft-Support bekommt, sollte am besten sofort auflegen und sich keinesfalls in ein Gespräch verwickeln lassen. Ist es doch passiert, und man ist nicht nur auf einen solchen Anruf eingegangen, sondern hat auch dem „Support“ Zugang zum Computer gewährt, muss dieser sofort vom Strom getrennt werden und durch einen vertrauenswürdigen Computer-Spezialisten überprüft werden. Sicherheitshalber sollten umgehend alle Passwörter und Zugangsdaten wie zu E-Mail-Konten, Online-Banking, Online-Shops ändern werden.

CEO-FRAUD UND DER GUTSCHEIN BETRUG

Eine weitere seit Jahren sehr erfolgreiche Betrugsmasche des Phishings mit ausgefeiltem Social Engineering ist das Übersenden von Gutschein-Codes an vermeintliche Vorgesetzte. Während sich bei einem Rechnungsbetrug die Kriminellen als rechtmäßige Zahlungsempfänger ausgeben und besonders die Mitarbeitenden der Buchhaltung gefährdet waren, Geld auf ein vermeintlich richtiges Konto zu überweisen, zielen die Gutschein-CEO-Fraud Angriffe auf die breite Masse aller Mitarbeitenden eines Unternehmens ab. Dieses Vorgehen verspricht den Angreifern eine höhere Erfolgschance. Das Vorgehen und die Zielgruppen werden von den Kriminellen ständig neu angepasst. Und neue Zielgruppen bedeuten für die Angreifer auch neue potenzielle Opfer. Während es die Kriminellen der Vergangenheit eher auf große Unternehmen abgesehen haben, stehen jetzt Unternehmen und Vereine ungeachtet der Größe im Visier.

Auch wenn die Ausführung variiert, bleibt die grundsätzliche Masche immer gleich. Der typische Verlauf beginnt mit einer Kontaktaufnahme. Kriminelle recherchieren im Vorfeld über soziale Netzwerke und Unternehmensseiten ihre Zielpersonen, häufig aber auch ein gesamtes Unternehmen. Anschließend schreibt die vermeintliche Geschäftsleitung die Mitarbeiter direkt an. Die Kommunikation wird entweder komplett per E-Mail geführt oder der Mitarbeitende wird gebeten, seine Mobilnummer für eine Kommunikation über WhatsApp zu übermitteln. Um zu verstehen, was diese Masche so erfolgreich macht, haben wir einen Selbstversuch gestartet. So kam es uns gelegen, dass am 31.12.2021 folgende Nachricht in den Postfächern einiger unserer Mitarbeitenden lag:

Hi Silvana,

Kindly let me know if you are free; I want you to get a task done for me urgently? am available via e-mail.

Nichts lag in dem Moment näher, als sich auf die Konversation einzulassen. Wir stellten es nicht in Frage, warum unser Geschäftsführer plötzlich englisch mit uns sprach und seltsame Dinge an einem arbeitsfreien Tag forderte. So antworteten wir am nächsten Tag, wie man helfen könne. Keine zehn Minuten später kam die erwartete Antwort:

I'm currently busy and I need some iTunes gift cards ASAP. I want you to help me getting iTunes gift cards from any nearby store or online store?

Reply me so that i will tell you the denomination required!

Nachdem wir uns also bereit erklärt hatten ihm zu helfen, folgten weitere Anweisungen.

Actually, what I need is € 1,000 worth of iTunes Gift Card (€100 or €500 denomination). You can get them from the Apple store and send me the picture of the cards after you get them scratched and also the receipt for expense report record…

Let me know if you can get it within20 mins time ?

Hier fällt besonders auf, dass die Kriminellen anfangen, einen Zeitdruck aufzubauen, damit dem Opfer keine Zeit bleibt, über die vielen Ungereimtheiten nachzudenken. Wir erklären dem vermeintlichen Geschäftsführer, dass am 1. Januar nur Tankstellen geöffnet haben und stellen uns hilflos. Auf eine Antwort müssen wir nicht lange warten:

Yes you can proceed to the gas station.
Thanks.

Jetzt war der Zeitpunkt gekommen, an dem wir testen wollten, wie weit wir mit Forderungen den Angreifer aus seinem vorgeschriebenen Konzept bringen konnten. Immerhin war gerade die Weihnachtszeit vorbei und so fragten wir unseren vermeintlichen Vorgesetzten, ob er uns nicht 150 Euro mit PayPal überweisen könnte:

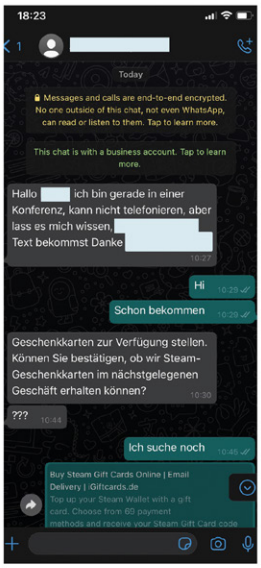
Dear Michael, as you know, I'm short on money, can you please immediately transfer some to my Paypal Account?
I need 150,- since I only have 850 left

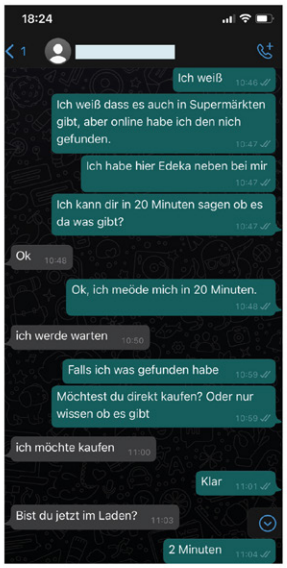
Auf die Antwort waren wir sehr gespannt. Der Angreifer zeigte Verständnis für unsere Situation, reduzierte den Wert der zu kaufenden Gutscheinkarten auf 800 € und erhöhte im gleichen Zug wieder den zeitlichen Druck:

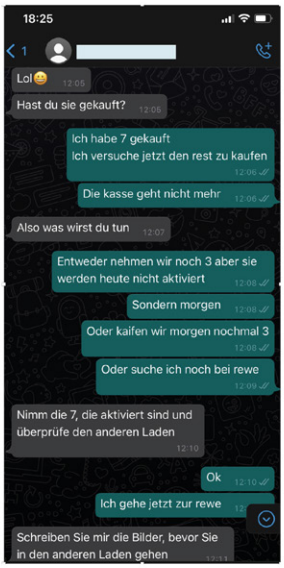
I understand and I'm also having some issues with my mobile transfer and as you know

- Die Kombination von Schein, Forderungen und der kontinuierliche Aufbau von zeitlichem Druck wirkt sehr einschüchternd. Daher ist es wichtig diese betrügerischen Absichten bereits von Anfang an zu erkennen, um den Angreifern keine Möglichkeit zu geben, ihre Ziele zu erreichen.

Gutscheinkarten-Masche







Schadenhöhe:
1.100,00 EUR

networker solutions GmbH

that there's a holiday today …
Kindly go ahead and purchase €800 iTunes gift card for me and sent to me ASAP!

I will appreciate if you can do that in a short time.

Es folgten in kurzer Zeit eine Vielzahl von Nachrichten, ob wir schon auf dem Weg wären und wann wir ihm die Gutscheine liefern könnten.

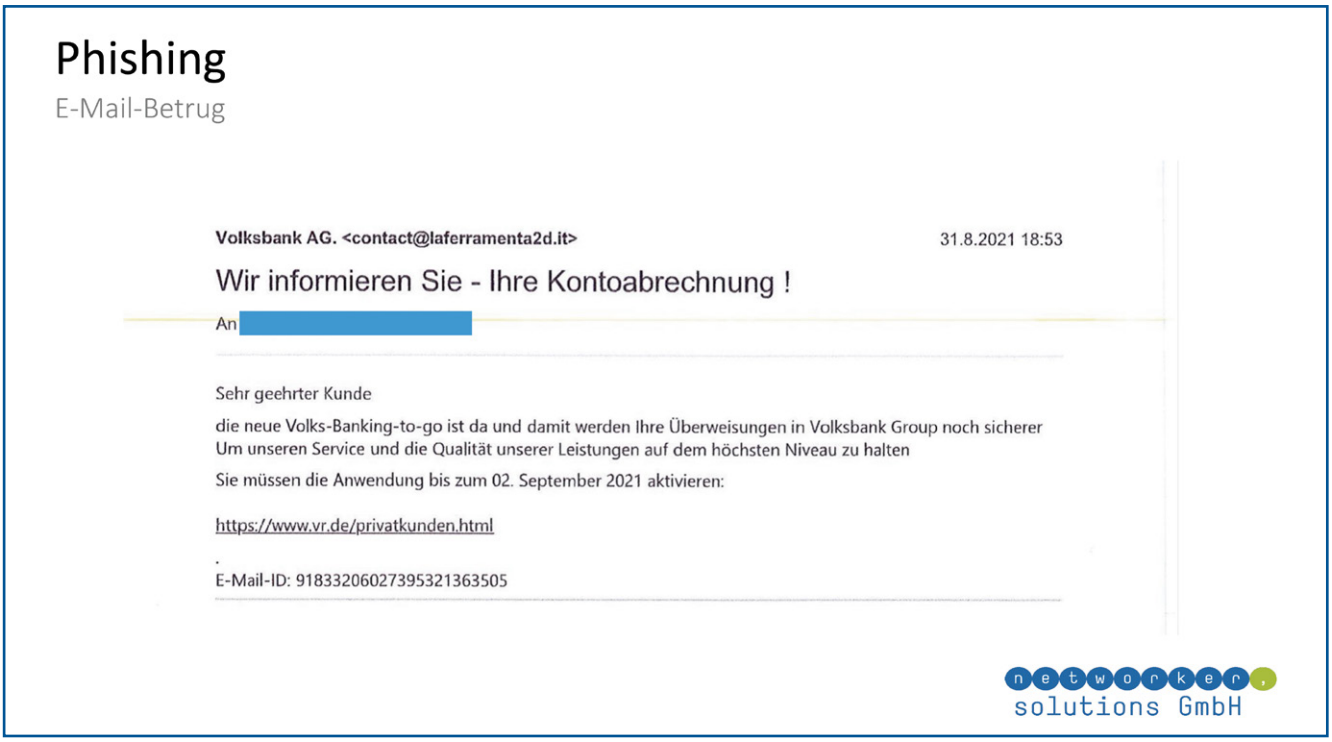
I will be waiting for your response…
Once you get the cards scratche them and send the pictures to me here ASAP !
Thanks.?

Wir führten diese Kommunikation noch einige Stunden weiter fort. Der Ton des Angreifers wurde dabei immer rauer und fordernder, seine Nachrichten immer kürzer, bis wir auflösten und ihm mitteilten, dass wir sein Spiel durchschaut hatten. Darauf verstummte sämtliche Konversation. Der Selbstversuch jedoch zeigte, warum diese Betrugsmasche, trotz vieler Ungereimtheiten, immer wieder erfolgreich ist. Die Kombination von Schein, Forderungen und der kontinuierliche Aufbau von zeitlichem Druck wirkt sehr einschüchternd. Daher ist es wichtig diese betrügerischen Absichten bereits von Anfang an zu erkennen, um den Angreifern keine Möglichkeit zu geben, ihre Ziele zu erreichen. Klassische Anzeichen, sind auffällige Betreffzeilen, unübliche Anreden, Vortäuschung von akutem Handlungsbedarf, schlechte Formulierungen, fehlende Umlaute, Links mit verdächtigen URLs, Anhänge in der E-Mail etc.

E-MAILS MIT SCHADSOFTWARE

Nicht in jedem Fall wollen Cyber-Kriminelle ihre Opfer mit Phishing zur Herausgabe sensibler Informationen oder personenbezogener Daten bewegen, sondern versuchen über diesen Weg Zutritt zu einem Unternehmensnetzwerk zu erlangen.

Dieses Vorgehen ist besonders tückisch, wenn der Absender der E-Mail offenbar jemand ist, den Sie kennen, mit welchem Sie bereits geschrieben haben und die Phishing- E-Mail auf einer vorhandene Konversation basiert. Dabei handelt es sich vorzugsweise um E-Mails mit angeblich wichtigen Dokumenten im Anhang oder Links zum Laden von Dateien aus dem Internet. Folgt man den Aufforderungen, läuft man Gefahr, sich unbemerkt einen Trojaner auf dem System zu installieren. Die Folgen eines solchen Trojaners reichen von der Kompromittierung des eigenen Rechners, einer Weiterverbreitung und Infektion von Dritten, bis hin zu einer folgenschweren Infektion des gesamten Unternehmensnetzwerkes. Dabei handelt es sich oft um Angriffe von Erpressergruppen. Nach dem Ausführen einer Datei aus einer solchen schadhaften Phishing-E-Mail bewegen sich diese



Cyber-Kriminellen oft Tage bis Monate unbemerkt im gesamten Unternehmensnetzwerk. Sie installieren ihre eigenen Programme, versuchen, oft erfolgreich, Schutzmaßnahmen zu umgehen, ziehen Daten ab, löschen Backups und verschlüsseln oftmals das gesamte Netzwerk. Die Folgen dieser Angriffe können immens sein. Betriebsunterbrechung, Produktionsausfälle, Datenverlust und Wiederherstellungskosten klettern hierbei schnell in Millionenhöhe. Zu berücksichtigen ist weiterhin ein möglicher Reputationsverlust, der den primären monetären Schaden langfristig übersteigen kann. Zudem besteht die Notwendigkeit einer professionellen Aufarbeitung des Vorfalls. Denn nicht selten befinden sich die Kriminellen noch im Netzwerk und beobachten ihre Opfer bei den Versuchen einer Schadenbehebung. Die Angreifer nutzen sämtliche erlangte Informationen und abgeflossene Daten, um die Betroffenen weiter zu erpressen. Wird das Lösegeld nicht bezahlt, weil man beispielsweise vorbildlich Offline-Backups besitzt, wird durch die Erpresser eine Veröffentlichung, der Versteigerung oder dem Verkauf sensibler Unternehmensinformationen angedroht.

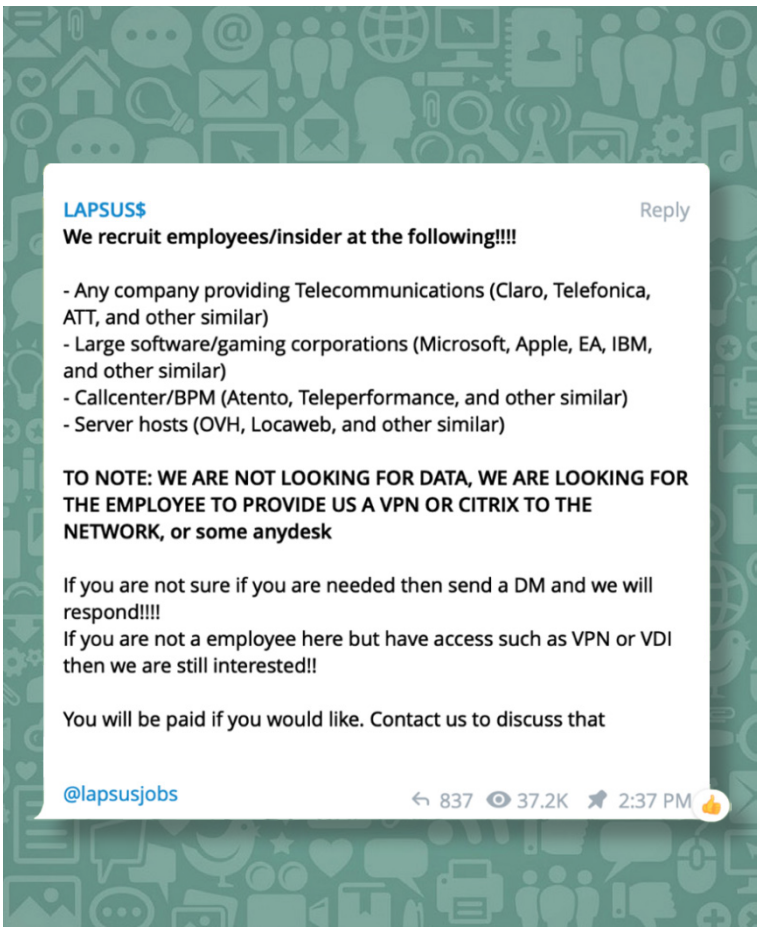
Diese sogenannte „zweifache" Erpressung findet seit einigen Monaten eine Erweiterung zu einer „dreifachen" Erpressung. Zusätzlich zur Verschlüsselung und Veröffentlichung von Daten und Informationen werden Familienmitglieder der Geschäftsleitung, Geschäftspartner und Kunden – jeder dessen Kontaktdaten die Erpresser in den Systemen erbeuten konnten – angeschrieben und auf den Vorfall mit Datenabfluss hingewiesen. Der Geschäftsführung des kompromittierten Unternehmens droht somit ein einschneidender Image-Verlust, der sich auch auf das private Umfeld ausdehnt. Die Erpresser nutzen dabei oftmals auch das Druckmittel „Datenschutzgrundverordnung", indem sie androhten, die Regulierungsbehörden über den erfolgten Datenabfluss zu unterrichten.
Von der Entdeckung einer Infektion bis zur fachgerechten Bereinigung der Systeme und einer Wiederherstellung der Arbeitsfähigkeit können je nach Unternehmensgröße, Ausmaß, Gefahrenbewusstsein und damit einhergehender Reaktionsbereitschaft mehrere Wochen bis Monate vergehen.

Für Unternehmen ohne vorherige Vorbereitung auf mögliche Cyberangriffe (Cyber Incident Response Readiness) kann zusammengefasst diese unbedachte Ausführung einer Phishing-E-Mail mit einem daraus resultierenden Ransomware-Angriff existenzbedrohend sein.

INSIDER-BEDROHUNGEN

Bei einer weiteren Ausnutzung des Faktors „Mensch" handelt es sich um sogenannte „Inside Jobs". Wie die Bezeichnung nahelegt, werden gezielt Insider, bei denen es sich beispielsweise um Mitarbeitende von Unternehmen handeln kann, angeheuert. Diese dienen als Handlanger den Angreifern als direkten Weg in die Netzwerke ihrer Arbeitgeber.

Ein eindrucksvolles Beispiel der letzten Monate liefert hierbei die Erpressergruppe Lapsus$. Seit ihrem Erscheinen in der Öffentlichkeit befand diese sich wiederholt in den Schlagzeilen, da Mitglieder dieser Gruppe erfolgreich Daten von prominenten Firmen wie Samsung, Nvidia, Ubisoft und Microsoft abgezogen und veröffentlicht hatten. Im Gegensatz zu den meisten Cyber-Kriminellen, die über verborgene Kanäle agieren, tritt Lapsus$ ungewohnt offen in sozialen Medien und Messangerdiensten auf. So publizierten sie auf mehreren Kanälen Stellengesuche, gerichtet an Mitarbeiter ausgewählter Zielunternehmen und Branchen. Statt aufwändig Schwachstellen in IT-Systemen zu suchen und auszunutzen oder auf eine erfolgreiche Phishingkampagne zu hoffen, bevorzugte Lapsus$



den direkten Weg mittels Zugangsdaten von Angestellten in das Netzwerk ihrer Opfer. Als Belohnung für Mitarbeiter, die bereit waren, Zugang zu ihren Unternehmen zu gewähren, bot Lapsus$ 20.000 US-Dollar pro Woche.

Wer sich erfolgreich gegen Cyber-Kriminelle zur Wehr setzen will, muss ihre Vorgehensweisen kennen. Social Engineering und Phishing bleiben ernstzunehmende sowie häufig unterschätzte Risikofaktoren in Unternehmen. Social Engineering wird immer dann eingesetzt, wenn Menschen beeinflusst werden können und es sich daraus Vorteile für Cyber-Kriminelle ergeben. Unternehmen sollten sich der hieraus resultierenden Gefahren bewusst sein. Der Schutz vor Cyberangriffen ist längst kein alleiniges Thema der IT-Abteilungen. Als eines der größten Geschäftsrisiken für Unternehmen bedarf es einer Kombination von technischen und organisatorischen Maßnahmen. Abschließend muss noch bemerkt werden, dass die letztendliche Verantwortung für die IT-Sicherheit und die daraus resultierenden Folgen die Geschäftsleitung trägt und dies auch nicht an die IT-Abteilung delegieren kann. Mithin ist die Aussage „aber mein IT-Leiter/meine IT-Leiterin hat doch gesagt…“ irrelevant. Die Geschäftsleitung tut also gut daran hin und wieder die getroffenen Maßnahmen von qualifizierten Dritten überprüfen zu lassen, deren Hauptgeschäft die Informationssicherheit ist und die sich nicht mit dem täglichen IT-Geschäft auseinandersetzen müssen, bzw. die Informationssicherheit „nebenbei“ betreiben.

Zertifikatslehrgang Cyber Insurance Manager*in

Silvana Rößler wird ab Herbst 2022 an der TH Dozentin beim Zertifikatslehrgang Cyber Insurance Manager*in, der unter der Leitung von Prof. Dr. Michael Fortmann (LL.M.) initiiert wurde.

Mit dem Zertifikatslehrgang Cyber Insurance Manager*in reagiert das Institut für Versicherungswesen (ivw, TH Köln) auf neue, hochdynamische Herausforderungen für die Versicherungswirtschaft, denn Cyber-Risiken gehören nach dem AGCS-Risk-Barometer aktuell zu den größten Geschäftsrisiken für Wirtschaft und Industrie. Deshalb befähigt die berufsbegleitende Weiterbildung Fach- und Führungskräfte dazu, Cyber-Risiken zu erkennen, zu bewerten und zu versichern.

Schwerpunkte liegen auf der Vermittlung technischer Hintergründe und dem Verständnis der IT-Forensik, dem Underwriting und der Produktgestaltung im Zusammenhang mit Cyber-Risiken. Teilnehmer*innen lernen, unterschiedliche Cyber-Risiken zu identifizieren, zu bewerten und ihre Auswirkungen unter Berücksichtigung IT-forensischer Erkenntnisse zu begrenzen. Zudem erfahren sie, welche präventiven Maßnahmen vorgenommen werden können, um den Eintritt von Cyber-Risiken zu verhindern und die IT-Sicherheit von Unternehmen zu erhöhen.

Anmeldeschluss für die Weiterbildung mit Start im November ist der 19. Oktober 2022 (max. 24 Teilnehmer*innen).

Weitere Informationen finden Sie unter:
www.th-koeln.de/CyberInsMan

Lernen Sie die Dozent*innen der Weiterbildung in unserer kostenlosen „Digitalen Sprechstunde“ kennen. Das Thema: Ransomware – eine Bedrohung für digitalisierte Unternehmen (Impulsvorträge sowie offenes Q&A am 18. Mai 2022).

Treffpunkte >> Ausblick

Bonn

4. Mai 2022, 18 Uhr

Gasthaus Nolden in Bonn-Endenich

13. Mai, 16 Uhr
(Eintreffen bis 15:45 Uhr)

Besuch der Limes-Ausstellung mit fachkundiger Führung im LVR-Landesmuseum in Bonn (Colmantstr. 14-16, 53115 Bonn). Nach dem Besuch im Museum Abendessen um 18 Uhr im DelikArt Restaurant (Colmantstr. 14-16, 53115 Bonn). Anmeldungen bitte an Günter Laux (Mail: guenter.laux@vvb-alumni.de)

Düsseldorf

12. Mai 2022, 18:30

Stammtisch in Brauerei Schumacher, Oststr. 123, 40210 Düsseldorf

Hamburg/Bremen/Oldenburg

27. April 2022, 18 Uhr

Stammtisch im Gasthaus an der Alster, Ferdinandstr. 65-67, 20095 Hamburg

Münster

5. Mai 2022, 17.30 Uhr

Der **Stammtisch** findet, wie bisher, bei Stuhlmacher, Prinzipalmarkt 6/7, 48143 Münster statt.

12.08.2022, 17:00 Uhr

Besuch der Andy-Warhol-Ausstellung im Picasso Museum Münster mit sachkundiger Führung. Anschließend gemütliches Abendessen im Caputo gehen. Anmeldungen bitte bis 10 Tage vor der Veranstaltung an Alfred Benecke (Mail: alfred.benecke@vvb-alumni.de)

Stuttgart

Nächster vorgesehener Termin:

30. Mai 2022 in Esslingen

TP Mannheim

Do 19. Mai 2022, 14:00-15:00 Uhr

„Revolution oder Rohrkrepierer – Versicherungslösungen im Paket (Embedded Insurance) - Impulsvortrag von Christian Gnam, Managing Director, Insurtech Hub Munich (ITHM)

Di 21. Juni 2022, 15:00-16:00 Uhr

„Wie ändert Kreislaufwirtschaft das Risiko- und Versicherungsmanagement? Neue Wege für Produktion und Absatz am Beispiel des Maschinen- und Anlagenbaus“ – Präsentation von Andreas Ellenberger, Co-Founder and CEO, Circonnact, und Circular Economy Enabler

Fachkreise >> Ausblick

Digitale Veranstaltungen

Rückversicherung / VVB Reinsurance Academy

Donnerstag, 21. April 2022

16:00 bis circa 17:30 Uhr per Zoom-Meeting

Eingeladen sind alle Mitglieder, Studenten sowie Gäste des Fachkreises Rückversicherung

Thema:

Strukturierte Rückversicherungslösungen

Für Mitglieder der WB ist die Anmeldung über die Homepage im internen Mitgliederbereich bis zum 18.04.2022 freigeschaltet. Unsere Gäste können sich mit einem E-Mail an Christian.Czempiel@vvb-koeln.de oder Jens.Ziser@wb-koeln.de anmelden.

Der Veranstaltungslink wird Ihnen kurzfristig vor der Veranstaltung übersendet. Bitte reservieren Sie sich den genannten Zeitraum.

CYBER

Dienstag, 26. April 2022

10:00 bis 12:30 Uhr per Zoom-Meeting

Eingeladen sind alle Mitglieder, Studenten sowie Gäste des Fachkreises Cyber.

Thema:

Rückenwind oder Gegenwind - Aktuelle Lage der Cyber Versicherung auf dem deutschen Markt

Agenda:

Siehe Hinweis im VVBmagazin 1/2022

IMPRESSUM

Herausgeber:
Vorstand der Vereinigung der Versicherungs-Betriebswirte e.V.
(Anschrift siehe Verlag)

Vorstand für Presse- und Öffentlichkeitsarbeit:
Stefan van Marwyk
Düsseldorfer Str. 135, 51063 Köln
redaktion@vvb-alumni.de

Redaktionsleitung:
Michaela Kolz
Bonner Str. 528c, 50968 Köln
michaela.kolz@vvb-alumni.de

Verlag:
Vereinigung der Versicherungs-Betriebswirte e.V. Geschäftsstelle
Frank Ackermann
Broichmühlenstr. 4, 50171 Kerpen
02237 52145
gs@vvb-alumni.de

Redaktionsteam:
Frank Ackermann, Wolfgang Franke, Nicole Gordine, Michaela Kolz , Jessica Krämer, Stefan van Marwyk, Markus Metzler, Sylvia Pirgiotis, Johanna Striowsky, Furkan Tatli, Gerd von Ullisperger

Internet-Adresse der VVB:
www.vvb-alumni.de

Redaktionsschluss:
für Heft 3/2022 ist am 15.05.2022.
Keine Haftung für unverlangt eingesandte Texte und Fotos. Die Redaktion behält sich vor, Artikel und Leserbriefe zu bearbeiten und zu kürzen.
Namentlich gezeichnete Artikel geben nicht unbedingt die Meinung der Redaktion wieder. Jeder Nachdruck muss durch die Redaktion genehmigt werden und ist honorarpflichtig. Zitate sind erlaubt, Belege davon erbeten.

Bezugspreis:
im Mitgliedsbeitrag der VVB enthalten, für Nichtmitglieder: Einzelpreis Euro 5,- zuzüglich Versandkosten.

Erscheinungsweise: 6 x jährlich

Gestaltung, Satz, Anzeigenservice und Gesamtherstellung:
Grafikhaus CGN KG
Augustinusstraße 11d, 50226 Frechen
02234 91195-0
02234 91195-10
redaktion@grafikhaus.de
Internet: www.grafikhaus.de