Handout zur Veranstaltungsreihe „Digitalisierungsinitiative für Mensch und Wirtschaft“

Das vorliegende Handout dient als inhaltliche Orientierung der insgesamt 14- teiligen Veranstaltungsreihe „Digitalisierungsinitiative für Mensch und Wirtschaft“, die zwischen Oktober 2021 und Mai 2022 durch das Regionalmanagement des Landkreises Dillingen a.d.Donau organisiert und durchgeführt wird. Aufgrund der pandemischen Situation wurden die bisherigen Veranstaltungen im Onlineformat durchgeführt. Das Regionalmanagement dankt allen beteiligten Referenten für Ihre lehrreichen Veranstaltungen.

Die kostenfreie Veranstaltungsreihe richtet sich an alle interessierten Bürgerinnen und Bürger, Unternehmerinnen und Unternehmer, insbesondere aus dem Landkreis Dillingen a.d.Donau. Bei Fragen, Anregungen und Wünschen können Sie sich gerne jederzeit an das Regionalmanagement des Landkreises Dillingen a.d.Donau unter regionalmanagement@landratsamt.dillingen.de wenden. Bei inhaltlichen Fragen stehen Ihnen ebenfalls die Referentinnen und Referenten der einzelnen Veranstaltungen zur Verfügung.

Das Regionalmanagement Dillingen a.d.Donau wird gefördert durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie.

Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

Regionalmanagement Bayern

Inhalt

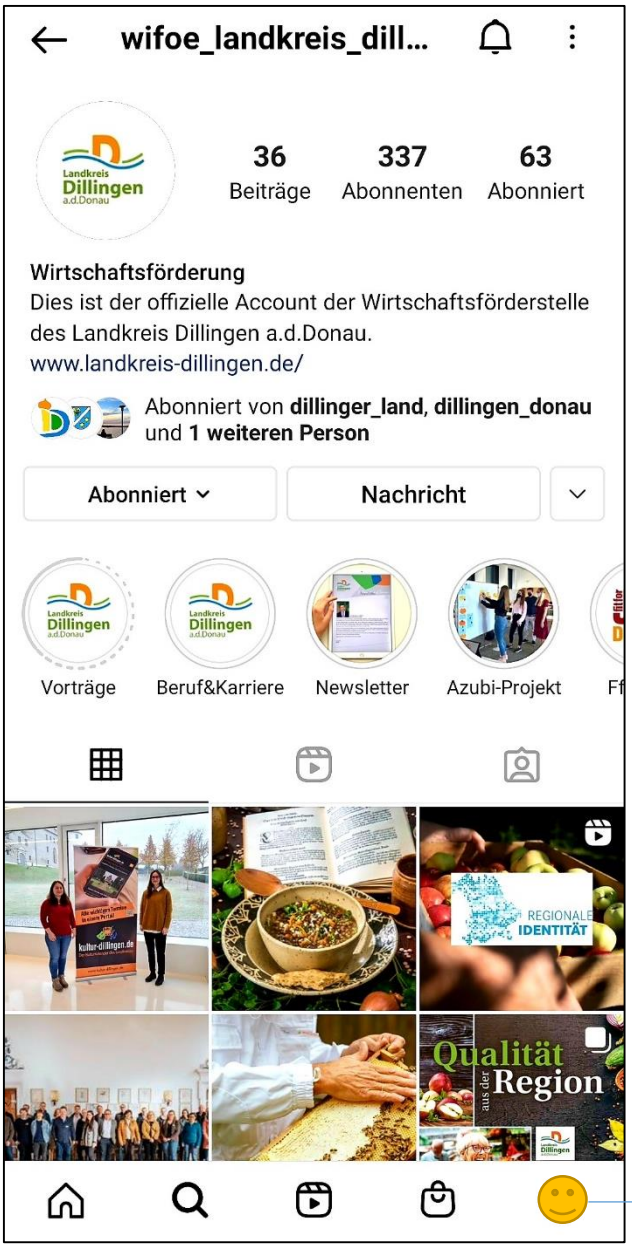
1.Veranstaltung: **„Instagram“** (21.10.2021) mit Olivia May, BayernLab Dillingen

Der Vortrag vom BayernLab Dillingen zum Thema Instagram wurde von insgesamt 30 Personen besucht. Es wurden in dem Onlinevortrag grundsätzliche Aspekte über das foto- und videofokussierte soziale Medium Instagram erläutert. Es werden von den Nutzern kostenfrei vielseitige Beiträge in Foto oder Videoform mit der Community, also den anderen Nutzern des sozialen Mediums, geteilt. Als Nutzer kann man sich ein eigenes Instagram- Profil anlegen, über das man eigene Bilder und Videos mit anderen, selbst ausgewählten Nutzern teilen kann. Es besteht die Möglichkeit, sich mit Freunden oder anderen Nutzern des sozialen Netzwerkes zu verknüpfen und ihnen zu folgen, um deren Beiträge zu sehen und entsprechende Kommentare dazu abgeben zu können. Im Jahr 2012 wurde das Netzwerk Instagram von Facebook gekauft. Weltweit nutzt über eine Milliarde Menschen das soziale Netzwerk, wobei die Hauptzielgruppe bei Menschen zwischen 13 und 30 Jahren gesehen wird.

Eine Nutzung von Instagram ist sowohl über Windows, als auch auf Smartphones mit Android und iOS möglich. Die App kann, je nach Gerät, über den Google Play Store, den App Store oder den Microsoft Store heruntergeladen werden. Für die Registrierung bestimmt man einen persönlichen Nutzernamen sowie ein Passwort. Die Angabe einer E- Mail - Adresse oder Handynummer sowie dem Geburtsdatum ist ebenfalls notwendig. Alternativ kann man sich auch über andere soziale Netzwerke wie Facebook oder Twitter auf Instagram anmelden. Als persönlicher Nutzername eignet sich insbesondere bei Unternehmen der Unternehmensname, um von anderen Nutzern bzw. Kunden gut gefunden werden zu können.

Der Startbildschirm, der bei Instagram auch „Nachrichten - Feed“ genannt wird, zeigt dem Nutzer zahlreiche Profile von Accounts, denen man als Abonnent folgt (vgl. Abbildung 1: Screenshot). Auch Themen, die einen grundsätzlich aufgrund anderer angesehener oder kommentierter Beiträge interessieren könnten, werden hier angezeigt. Am Smartphone wird im unteren Bereich der App eine Leiste mit verschiedenen Symbolen angezeigt. Drückt man das Haussymbol, landet man in dem Nachrichten- Feed. Mit der Lupe rechts neben dem Haus kann man Accounts oder nach bestimmten Themen suchen. Mittig ist eine Filmkassette abgedruckt. Hier gelangt man zu den sogenannten „IGTV - Videos“. Hier können auch längere Videos, wie etwa Dokumentationen oder Berichte präsentiert werden. Rechts daneben

befindet sich ein Taschensymbol, hinter diesem verbergen sich Instagram- Stores. Über die Stores, also Läden, können Händler bzw. Nutzer Ihre Ware bewerben und verkaufen. Ganz rechts auf der abgebildeten Leiste gelangt man zu seinem eigenen Profil. Dies ist dann relevant, wenn man Informationen über sich bearbeiten möchte.



Nutzername

Profilbild

Profilbeschreibung, individuell gestaltbar, gut für die wichtigsten Informationen

Möglichkeit zum direkten Austausch mit dem Profil

Gespeicherte Story - Highlights

Verschiedene Beiträge, in Foto- und Videoform

Eigenes Profil

Abbildung 1: Instagram Account der Wirtschaftsförderung (Quelle: eigene Darstellung)

Nachrichten-feed

Suchfunktion

IGTV-Videos

Instagram-Stores

Es existieren einige weitere Grundfunktionen außer dem Hochladen von Bildern in dem Medium. Es steht den Nutzern eine Vielzahl von Filtern zur Verfügung, mit denen

Bilder einfach bearbeitet werden können. Zudem kann beispielsweise Musik hinterlegt werden, Text auf Bilder gedruckt werden, Standorte angegeben oder Sticker auf Bilder gepostet werden. Das sind nur einige wenige Möglichkeiten, um seinen Inhalt zu verschönern. Nutzer haben die Möglichkeit, eine Art Blog auf ihrem Account zu gestalten. Auch können Reels gestaltet werden. Bei Reels handelt es sich um kurze Videos, in denen man Inhalte produzieren und veröffentlichen kann. Als Nutzer besteht zudem die Möglichkeit, in einer Story bestimmte ausgewählte Inhalte für eine begrenzte Dauer von 24 Stunden für einen vorher festgelegten Nutzerkreis zu veröffentlichen.

Nicht nur für Privatpersonen bietet Instagram verschiedene Funktionen an, sondern auch für Unternehmen. Es wird bei einem professionellen Konto unterschieden zwischen der Option Business und Creator. Für die meisten Unternehmen sind Businessprofile wohl die geeignetste Option. Ein Unternehmensprofil verfügt über einen erweiterten Funktionsumfang als ein Privatprofil. Durch ein professionelles Profil besteht zusätzlich beispielsweise die Möglichkeit zu sehen, wie viele Personen das Profil benutzt haben, wer diese Personen sind, sodass man sein Angebot auf die angesprochenen Personengruppen anpassen kann. Man kann als Unternehmen über Instagram gezielt für einen bestimmten, für sich abgestimmten Nutzerkreis Werbung schalten. Um die persönliche Erreichbarkeit zu fördern, besteht die Möglichkeit, seine Kontakte mit Telefonnummern zu teilen.

Für weitere Informationen steht das BayernLab allen interessierten Personen für einen persönlichen Besuch nach Terminvereinbarung kostenfrei zur Verfügung.

2. Veranstaltung: **„Muss es immer Bargeld sein? Schritt für Schritt zur Kartenakzeptanz“** (27.10.2021) mit Dr. Ernst Stahl, Mittelstand 4.0 – Kompetenzzentrum Augsburg

In dem Webinar wurden nach einleitenden Worten über die Ausgangslage des Zahlens einige Fakten über das Bezahlen erläutert, die in Abbildung 2 veranschaulicht werden. Klassische Zahlungsverfahren sind neben der Vorkasse, Rechnungszahlung, Lastschrift sowie Nachnahme auch Kartenzahlungsverfahren in der stationären Nutzung. Kartenzahlungsverfahren lassen sich in zwei unterschiedliche Arten kontaktbasiert und kontaktlos unterteilen.

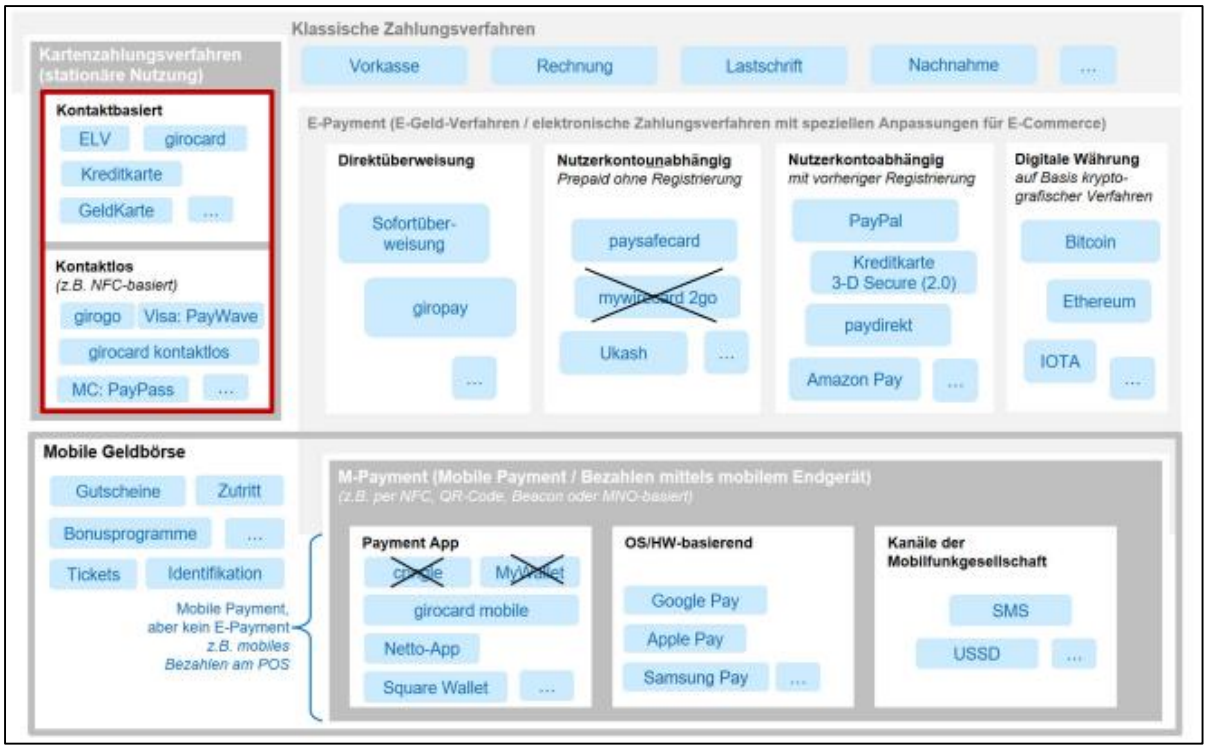


Abbildung 2: Übersicht über Zahlungsverfahren (Quelle: ibi research 2020)

Der Referent betont, dass häufig der „Kartendurchblick“ bei der Bevölkerung und dem Handel nicht vorhanden ist und das Bezahlverhalten in Deutschland per Bargeld im Vergleich zu anderen Ländern wie etwa Schweden sehr beliebt ist.

Die Corona- Pandemie hat aufgrund von Hygieneaspekten und dem einzuhaltenden Abstand zu anderen Menschen, aber auch Zukunftsängsten und Traumata bei den Kunden und Verkäufern direkte Auswirkungen auf den Zahlungsverkehr und auf das Bezahlverhalten. Das Zahlverhalten änderte sich jedoch in Deutschland, auch im internationalen Vergleich gesehen, nur langsam.

Kartenzahlungen sind als einfach, sicher und hygienisch, insbesondere für die Kassierenden, zu bewerten. Während die klassische Bankkarte im Jahr 2020 bei 81,8 % der bargeldlosen Zahlungen verwendet wurde, fielen 16,6 % auf klassische Kreditkarten bzw. Debit-„Kreditkarten“. Kontaktloses Zahlen erfolgte im Jahr 2020 bei über 60 % der gesamten Kartenzahlungen. Diese sind noch unkomplizierter, schneller und hygienischer, sofern sie ohne PIN Eingabe auf den Touchpads funktionieren.

Ein Blick auf die Geschwindigkeit der verschiedenen Bezahlverfahren ist lohnenswert. Während eine Barzahlung im Schnitt mit 24 Sekunden am längsten dauert, ist eine girocard Zahlung mit PIN Eingabe mit 23 Sekunden nur marginal schneller. Eine

kontaktlose girocard Zahlung hingegen ist mit 11 Sekunden im Schnitt jedoch deutlich am schnellsten.

Insgesamt verzeichnet girocard ein starkes Wachstum mit anhaltendem Wachstumstrend auch trotz Corona. Ebenfalls wurde „mobiles Bezahlen“ per digitalisierter Karte und bereits bestehenden Möglichkeiten wie Apple Pay, Google Pay und Samsung Pay mit dem Smartphone im Vortrag ausführlich diskutiert. Diese kontaktlosen Zahlungsarten sind als komplett hygienisch und schnell zu kategorisieren.

Trotz der Vorteile der Kartenzahlung bleibt festzuhalten, dass Bargeld, etwa aus Datenschutzgründen, durchaus wichtig ist und auf absehbare Zeit nicht verschwinden wird, denn Bargeld ist laut Ernst Stahl gelebte Freiheit und ein vollständiger Verzicht erscheint als nicht sinnvoll.

Im Online- Handel gibt es eine Vielzahl unterschiedlicher Zahlungsverfahren und die Auswahl gilt es aufgrund des Spannungsfeldes „Kosten für den Händler“ und „Akzeptanz durch den Kunden“ gut zu überlegen.

3.Veranstaltung: **„Social-Media-Marketing für Einzelhandel, Handwerk und Dienstleister“** (09.11.2021) mit Manuel Schuster, Werbeagentur Schuster, Wirtschaftsjunioren

In den sozialen Medien, wie Facebook, Instagram, WhatsApp, YouTube, Snapchat, Twitter oder TikTok, aber auch LinkedIn, Xing oder Pinterest können sich Menschen miteinander vernetzen, gemeinsam kommunizieren und verschiedenste Inhalte austauschen und posten. Weltweit nutzen über 500 Millionen Nutzer täglich sogenannte soziale Medien. Jeder Mensch verfügt im Durchschnitt über 8,5 Accounts und nutzt im Schnitt 144 Minuten pro Tag soziale Medien. Verschiedene Altersgruppen nutzen tendenziell unterschiedliche soziale Medien, was bei der Bestimmung von Zielgruppen essentiell sein kann. Es ist möglich, preiswertes Marketing für Unternehmen zu betreiben, ohne dass es von den Nutzerinnen und Nutzern zu bewusst als Werbung wahrgenommen wird. Es gibt einen sogenannten Social- Media-Kreislauf, wobei für die Kommunikation mit Kunden verschiedene Inhalte geplant werden müssen, danach Texte sowie Bilder als Inhalte erstellt werden, um diese auf Websites, in den sozialen Medien, aber auch auf anderen Plattformen zu verteilen. Es

ist sehr sinnvoll, eine Erfolgskontrolle der Maßnahmen durchzuführen, und diese zu analysieren, um wiederum in Kommunikation mit den Kunden zu kommen und den Kreislauf zu wiederholen. Im Vortrag wurde der Zusammenhang zwischen Erwartungshaltung und Begeisterung von Kunden erläutert. Um Neukunden zu gewinnen, benötigt man überzeugte Kunden. Als häufigster Grund für Kundenverluste wurde vom Referenten der Aspekt des Gefühls der fehlenden Wertschätzung von Kunden selbst genannt.

Des Weiteren ist es für Unternehmen empfehlenswert, ihre Google- Bewertungen regelmäßig zu pflegen. Als Unternehmer lohnt es sich, entsprechende Business Accounts zu nutzen, da diese verschiedene, integrierte Analysemöglichkeiten mit sich bringen, von denen man als Unternehmer profitieren kann.

Um möglichst viel Erfolg zu erzielen, ist neben einem sogenannten Content-Plan, also die Festlegung zu welchem Zeitpunkt welcher Inhalt in welcher Form auf welcher Plattform gepostet werden soll, die Definition von klaren Zielen relevant. Es kann hilfreich sein, verschiedene Soziale Medien Kanäle gegenseitig zu bewerben, beispielsweise mit Hilfe der Nutzung von QR Codes. Um sich weiterzuentwickeln, ist das Einholen von Inspirationen elementar. Besonders aufzupassen gilt es bei Schleichwerbung oder Werbung ohne die entsprechende Kennzeichnung. Auch Aspekte wie Impressum und Datenschutzerklärungen sind auf den Profilen erkennbar zu positionieren.

Um die Reichweite eines Profils zu erhöhen, gilt es stetig, das eigene Profil zu optimieren und in Interaktion mit anderen ähnlichen Profilen zu gelangen. Ein aktiver Austausch mit den eigenen Followern, also Personen die dem eigenen Profil folgen und die entsprechenden Inhalte automatisch angezeigt bekommen, ist nicht zu unterschätzen, ebenso wie die aktive Verwendung von Hashtags und Ortsangaben. Das regelmäßige Produzieren und Posten von Inhalten ist relevant, wobei es wichtig ist, dass die Inhalte einen entsprechenden Mehrwert bieten und aktuelle Trends, wie etwa Challenges aufgegriffen werden.

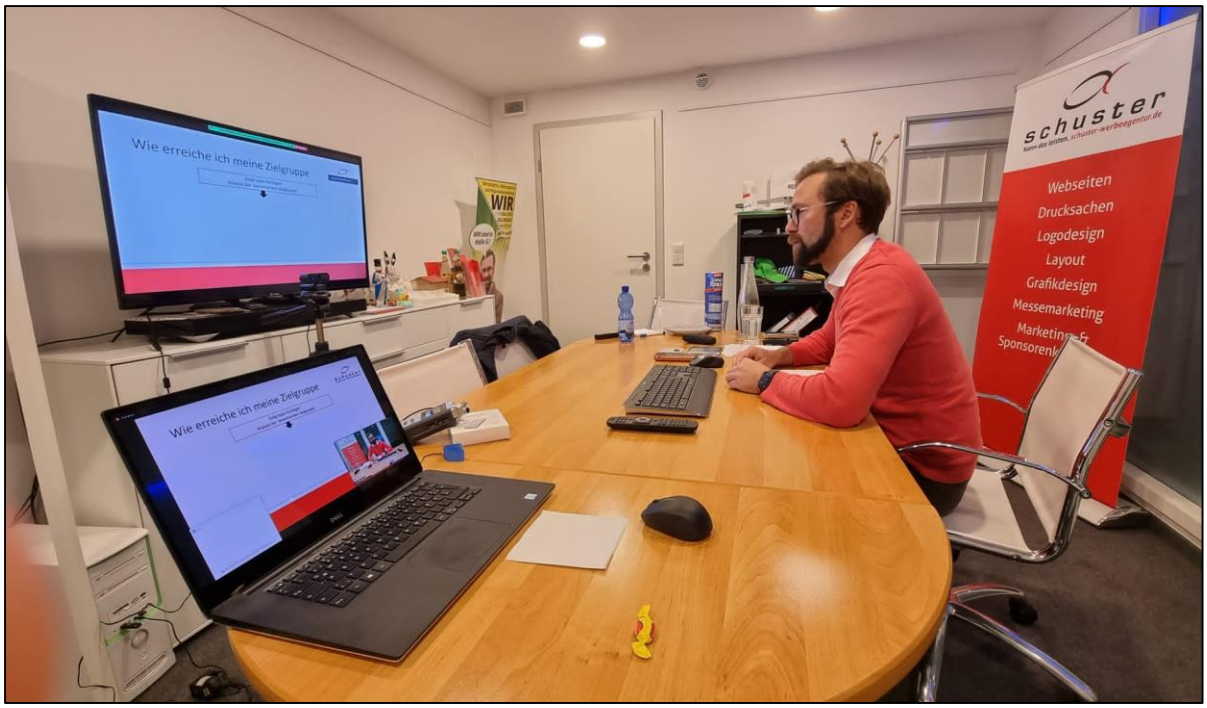


Abbildung 3: Herr Schuster während der Onlineveranstaltung (Quelle: Manuel Schuster)

4.Veranstaltung: **„Der Weg zur eigenen Webseite für kleine und mittelständische Unternehmen“** (16.11.2021) mit Manuel Schuster, Werbeagentur Schuster, Wirtschaftsjunioren

Nach der Frage und Aufführung von vielseitigen Gründen, warum man eine Webseite haben sollte, wurden Aspekte wie optische, inhaltliche und technische Merkmale genannt, weshalb sich eine (neue) Webseite lohnen kann (vgl. Abbildung 4). Es gibt mehrere Möglichkeiten, Webseiten zu erstellen. Über einen Dienstleister können einzelne Elemente Abschnitt für Abschnitt implementiert werden oder alternativ vorgefertigte Templates verwendet werden, sofern man die Webseite selbst gestalten möchte. Alternativ kann man eine Agentur beauftragen, die diese Aufgaben für einen übernimmt. Um die Entscheidung zu treffen, für welche Art man sich entscheidet, lohnt es sich, sich Gedanken darüber zu machen, wie viel man in dem Moment selbst zu tun hat, ob man über die entsprechenden Skills verfügt, derartige Schritte zu gehen und ob man ein gewisses Budget zur Verfügung hat, welches man für die Erstellung einer Webseite verwenden kann oder möchte. Es sind zwei Ansätze zu unterscheiden, einmal die Programmierung einer Webseite mit webgeeigneten Programmiersprachen wie CSS, HTML oder JavaScript oder der zweite Ansatz mit Hilfe von WordPress, wobei Themes und Plugins sowie Inhalt implementiert werden. Bei einem individuellen

Layout, das nach Corporate Design (CI und CD) inklusive einer Logo Integration gestaltet wird, und sehr zielgruppenorientiert designt werden kann, etwa barrierefrei, mit gut sichtbarer Telefonnummer oder bestimmten Inhalten wie aktuellen Veranstaltungen oder speziellen Produkten, ist eine sinnvolle Menüstruktur notwendig. Vorbereitete Layout- Templates hingegen sind endgeräteoptimiert, betriebssystemoptimiert, SEO optimiert, zudem updatefähig und nachträglich änder- und erweiterbar. Ein großer Vorteil liegt in der individuellen Anpassbarkeit.

Abbildung 4: Wortwolke (Quelle: Manuel Schuster)

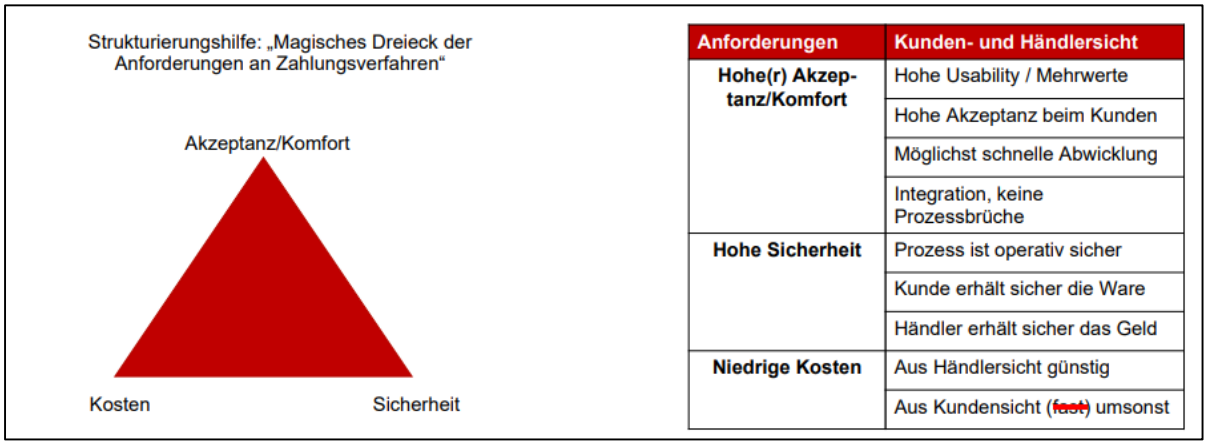
Auch die Frage, wie man eine individuelle Adresse im Internet, eine sogenannte Domain erhält, wurde Schritt für Schritt erläutert. Zudem wurden Tipps für die Überlegungen einer geeigneten, praktischen Domain erläutert. Nach den Überlegungen gilt es, einen für sich geeigneten Host bzw. Provider auszuwählen. Gerade im Bereich des Hostings gibt es viele Agenturen mit Full- Service, was wiederum sehr bequem sein kann. Im weiteren Vorgehen überprüft man die Verfügbarkeit seiner gewählten Domain und beantragt die Wunschadresse beim Provider. Danach erfolgt eine Reservierung dieser Domain.

Wie bei den meisten Dingen gilt, günstig, schnell und qualitativ hochwertig klappt nicht zusammen. Es müssen Abstriche gemacht werden. Es wurden mehrere Kostenübersichten für die verschiedenen Varianten gezeigt, um eine grobe Vorstellung zu erhalten.

5.Veranstaltung: **„Auswahl und Integration von Zahlungsverfahren in Ihrem Online-Shop“** (18.11.2021) mit Dr. Ernst Stahl, Mittelstand 4.0 - Kompetenzzentrum Augsburg

Es wurden durch den Referenten die Vor- und Nachteile der verschiedenen Zahlungsverfahren sowohl für Kunden als auch für Händler detailliert diskutiert. Neben den klassischen Zahlungsverfahren auf Rechnung, per Vorkasse, Lastschrift und Kreditkarte wurden weitere ausgewählte Verfahren wie PayPal, Ratenkauf, giropay + paydirekt = giropay, Amazon, Klarna Sofortüberweisung und neue Verfahren der Mobiltelefonbetriebssystementwickler wie Apple Pay und Google Pay diskutiert. Als Strukturierungshilfe kann das sogenannte „Magische Dreieck der Anforderungen an Zahlungsverfahren“ helfen (vgl. Abb.5). Die drei Eckpunkte sind Kosten, Sicherheit sowie Akzeptanz bzw. Komfort. Jede dieser drei Anforderungen gilt es sowohl aus Händler-, als auch aus Käufersicht zu beachten.

Zusammenfassend ist festzuhalten, dass Endkunden die entstehenden Kosten für die Händler (meist) egal sind und das Bezahlen für den Kunden primär schnell und einfach funktionieren muss. Das eine perfekte Zahlungsverfahren für Händler und Kunden gibt es nicht, weshalb es sich anbietet, dass ein Händler mehrere Zahlungsverfahren in seinem Shop anbietet, um die Abbruchquote von Käufen möglichst niedrig zu halten. Es ist wichtig, dass Händler neben der reinen Conversion- Betrachtung nicht die Kosten einzelner Zahlungsverfahren aus den Augen verlieren. Durch die starke Kundenauthentifizierung ändert sich die Usability im Checkout zum Teil erheblich, es führt zu starken Auswirkungen auf Abbruch- und somit Nutzungsquoten, weshalb eine geschickte Gestaltung essentiell ist.



Anforderungen	Kunden- und Händlersicht
Hohe(r) Akzeptanz/Komfort	Hohe Usability / Mehrwerte
	Hohe Akzeptanz beim Kunden
	Möglichst schnelle Abwicklung
	Integration, keine Prozessbrüche
Hohe Sicherheit	Prozess ist operativ sicher
	Kunde erhält sicher die Ware
	Händler erhält sicher das Geld
Niedrige Kosten	Aus Händlersicht günstig
	Aus Kundensicht (~~fast~~) umsonst

Abbildung 5: Magisches Dreieck (Quelle: ibi research – E commerce – Leitfaden)

6.Veranstaltung: **„Ransomware: Aktuelle Bedrohungen und Vorgehen der Kriminellen“** (23.11.2021) mit Prof. Dr. Lothar Braun, Hochschule Augsburg

Nach einigen aktuellen Beispielen von Ransomware - Angriffen bei verschiedensten Unternehmen wurde vom Referenten ein einführender Überblick zum Thema Malware gegeben. Das Wort „Malware“ ist eine Wortzusammensetzung aus „Malicious Software“, und bedeutet so viel wie bösartige Software. Es existiert eine Vielzahl unterschiedlicher Arten von Malware, jedoch ist allen gemeinsam, unerwünschte Aktionen auf dem System des Opfers durchzuführen. Während Computerviren, Würmer und Trojanische Pferde die Verbreitungswege von Malware beschreiben, handelt es sich bei Adware/Scareware, Spyware/ Keylogger, Bot und Ransomware um bösartige Funktionen.

Computerviren existieren bereits seit den 1970er/80er Jahren und wurden lange Zeit ohne direkte kriminelle Absichten entwickelt und erzeugt. Eine infizierte ausführbare Datei wird auf einem neuen System ausgeführt und durchsucht das ganze Dateisystem nach anderen Dateien, wobei sie sich selbst in neue Dateien einfügt.

Würmer verbreiten sich autonom meist über das Netzwerk, also über E-Mail oder Netzwerkverbindungen. Es wird nach verwundbaren Systemen gesucht. Die Würmer verbreiten sich dann automatisch.

Bei Trojanischen Pferden, oder auch Trojanern genannt, handelt es sich um Schadsoftware, die sich als legitimes Programm ausgibt. Der Nutzer bezieht ein Programm aus dem Internet oder erhält eine E-Mail und installiert dieses Programm. Wenn das Programm gestartet wird, wird parallel dazu eine bösartige Funktion gestartet. Grundsätzlich besteht die Möglichkeit, dass ein Trojaner auch ein Dokument ist, oder die Optik eines Dokumentes aufweist. Ein klassischer Weg eines Trojaner-Befalls ist es, dass ein Nutzer eine E-Mail mit einem Word-Dokument inklusive der Bitte um Aktivierung der „Editier-Funktion“ dieses Dokuments erhält. Hierüber wird ein Makro-Code inkl. des Schadcodes ausgeführt.

Sogenannte Adware zeigt Werbung auf dem Bildschirm an und öffnet Fenster mit unerwünschten Inhalten. Kriminellen gelingt es Geld durch Anzeige von Werbung oder durch Kauf durch den Nutzer zu erhalten.

Scareware beinhaltet, wie ebenfalls durch den Namen deutlich wird, angstmachende Botschaften, die zum Kauf von Software verleitet. Hierbei verdienen die Kriminellen

auf diese Weise Geld durch den Nutzer. Es besteht auch die Möglichkeit von Scareware durch Webseiten, wobei diese zur Installation anderer bösartiger Software verleiten.

Spyware/ Keylogger spionieren infizierte Systeme aus. Sie stehlen beispielsweise Nutzernamen und Passwörter, indem es zum Einsatz von Mitschnitten von Tastatureingaben kommt. Des Weiteren werden gespeicherte Passwörter oder sonstige Dateien im Browser ausgelesen. Häufig kommt es zur Exfiltration von Account- und Finanzdaten, so werden Kreditkartendaten sowie Kontoinformationen und Zugänge zu Onlinebanking ausspioniert. Die auf diese Weise gesammelten Daten werden dann für Betrug genutzt, etwa für Einkäufe per Kreditkarte im Internet, aber auch für Identitätsdiebstähle.

Ransomware verschlüsselt Daten auf Systemen, wobei legitime Nutzer nicht mit dem System arbeiten können und nicht auf wichtige Daten zugreifen können. Der Ransomware- Betreiber bietet möglicherweise einen Schlüssel zur Entschlüsselung gegen Geldzahlung an. Die Zahlungen sollen meistens über digitale Kanäle wie Bitcoins erbracht werden. Zusätzlich zu diesem Vorgehen kopieren die Erpresser Daten vor der Verschlüsselung seit jüngerer Vergangenheit und drohen mit einer Veröffentlichung der Daten im Internet. Auf diese Weise erpressen Sie Geld vom Datenbesitzer. Auch ein Lösegeld für die Entschlüsselung der verschlüsselten Daten und der Androhung geheime Daten im Internet zu veröffentlichen, ist üblich. Grundsätzlich besteht die Möglichkeit einer Verbreitung der Ransomware über verschiedene Kanäle. Klassischerweise wird Ransomware als Trojaner verbreitet, indem der Nutzer zur Installation des Trojaners verführt wird, etwa durch Spam-Emails, die eine EXE Datei oder ein Word- Dokument im Anhang hat. Eine automatische Verbreitung kann als Wurm durch das Ausnutzen von Schwachstellen in nicht-aktualisierter Software oder Fehlkonfigurationen passieren. Hierbei werden Zugangsdaten zu Servern erraten. Als bekannte Beispiele sind WannaCry und NotPetya zu nennen. Der Referent spielte diese beiden Beispiele als Demovariante während des Vortrags ab. Neuere Entwicklungen sind durch das manuelle Aufbringen von Ransomware durch Hackergruppen festzustellen. Hacker dringen hierbei in Computernetzwerke ein, etwa durch Schwachstellen und installieren manuell Ransomware.

Einige Beispiele für die typische Verbreitung mit dem Ziel des End-Nutzes sind etwa CryptoLocker in den Jahren 2013-2014 oder Locky im Jahr 2016.

Aus Sicht des Digitalverbandes BitKom ist die Summe der Schäden durch Cyberangriffe für die deutsche Wirtschaft auf eine Höhe von 220 Milliarden Euro festzulegen. Größter Treiber der Entwicklung ist neben der Erpressung durch Ransomware auch ein Ausfall von Systemen, beispielsweise in der Produktion, als Teil der Ransomware- Angriffe.

Ransomware- Angriffe sind in zwei Arten zu unterscheiden. Neben einfachen Angriffen, bei denen Ransomware per E-Mail bzw. Schwachstelle verteilt wird und der Angriff direkt nach Ausführung der Malware beginnt, existieren komplexe Angriffe, bei denen nach einer initialen Infektion über eine Schwachstelle der Angreifer sich auf das Ziel verbindet und das Opfer auf dessen Lohnenswert überprüft.

Als neuer Trend ist Ransomware-as-a-Service zu nennen. Hierbei handelt es sich um Gruppen wie REvil und Dark Side, die Erpressern Software und Infrastruktur anbieten. Erpressern ist es möglich, sich Dienste zu mieten und damit Ransomware- Angriffe durchzuführen.

Da zunehmend Privatpersonen und Firmen Ziele von Ransomware sind, da Kriminelle durch automatisierte Software verhältnismäßig einfach Geld verdienen können, gilt es sich zu schützen. Neben präventiven Maßnahmen, wie einer Verbesserung der IT–Sicherheit, um Ransomwaregruppen den Einbruch schwerstmöglich zu gestalten, ist eine Vorbereitung von Backups empfehlenswert, um Datenverluste im Falle eines Angriffes wiederherstellen zu können. Als reaktive Maßnahmen nach einem Angriff sind das Einspielen von Backups sowie ein Versuch der Wiederherstellung von verschlüsselten Daten sinnvoll.

7. Veranstaltung: **„Suchmaschinenoptimierung, Google- Anzeigen und Social-Media- Kampagnen“** (24.11.2021) mit Manuel Schuster, Werbeagentur Schuster, Wirtschaftsjunioren

Im Rahmen des Vortrags sollte geklärt werden, welchen Einfluss man selbst auf die Einblendung der eigenen Website bei den Suchanfragen hat. Des Weiteren wurden Grundlagen über bezahlte Werbung bei Suchmaschinen und Social- Media- Portalen erläutert und Tipps gegeben, wie man Werbebudget sinnvoll einsetzen kann und im Anschluss den Erfolg einer Kampagne messbar machen kann. Für die Optimierung einer Website ist es zunächst notwendig, den Ist- Zustand zu ermitteln und daraus abzuleiten, welche Inhalte oder Strukturen man verbessern möchte. Auch durch die richtige Platzierung von Schlüsselwörtern, sogenannte Keywords, die im Optimalfall auch in der Domain zu finden sind, kann man die Optimierung vorantreiben. Auch durch Link Building, also Verlinkungen der Seite zu qualitativ hochwertigen Artikeln, die regelmäßig auf ihre Aktualität überprüft werden, kann man Optimierungen betreiben. Durch das Verfassen von Gastbeiträgen auf anderen Seiten oder das Versenden von Pressemitteilungen kann man ebenso wie durch gezielten, gut geplanten Linkaustausch sogenannte Backlinks, also Links von anderen Seiten auf die eigene Seite erzielen. Die gezielte Positionierung von Keywords auf jeder Seite kann zur Optimierung der Website beitragen.

Bezüglich der bezahlten Werbung wurde beispielhaft an Google Ads und Instagram erläutert, welches Vorgehen man verfolgen muss. Aktuell kann man bei Google Ads aus insgesamt sieben unterschiedlichen Kampagnenformaten, wie etwa Suchkampagnen, Shopping- Kampagnen oder Video- Kampagnen, die für sich am geeignetste Kampagne auswählen.

Bei Instagram Kampagnen verfolgen Unternehmen verschiedene Ziele, wie etwa Branding Effekte, um die Unternehmensbekanntheit zu erhöhen, die direkten Klickzahlen auf der Website zu vergrößern oder auch Sales zu steigern. Es empfiehlt sich eine Verknüpfung mit Facebook, da die Werbeanzeigen dann auf beiden Plattformen gleichzeitig beworben werden können, ohne einen Mehraufwand zu haben.

Je nach Branche ist eine differenzierte Vorgehensweise empfehlenswert. Im Allgemeinen gilt es, sich Gedanken über die Höhe des Budgets zu machen, bevor man eine Kampagne startet. Insbesondere sogenannte Smart Kampagnen bergen ein

hohes Gefahrenpotenzial. Grundsätzlich gilt es zu bedenken, den Erfolg der eigenen Werbekampagne mit Hilfe von Analysetools messbar zu machen.

8. Veranstaltung: **„Schutzmaßnahmen gegen Ransomware“** (30.11.2021) mit Prof. Dr. Lothar Braun, Hochschule Augsburg

Der Vortrag behandelte schwerpunktmäßig verschiedene Schutzmaßnahmen, die sowohl präventiv, als auch reaktiv gegen Ransomware zur Verfügung stehen. Zunächst wurde aber auch darauf eingegangen, was man unter Ransomware versteht, wie sie sich verbreitet und dies wurde dann an einem praktischen Demobeispiel von dem Referenten aufgezeigt.

Ransomware verschlüsselt Daten auf dem System, sodass der Nutzer nicht mehr richtig damit arbeiten kann. Die Verbreitung der Ransomware erfolgt dabei klassisch über zwei Wege, zum einen in Form von Trojanern, und zum anderen in Form von sogenannten Würmern. Die Kriminellen fordern im Folgenden eine Geldsumme, die bezahlt werden muss, um entweder die Daten wieder zu entschlüsseln oder um die Veröffentlichung der Daten zu verhindern. Wie Ransomware ein Gerät befallen kann, wurde dann anschaulich an einem Demobeispiel gezeigt.

Im letzten und umfassendsten Teil des Vortrags ging es dann darum, wie man sich vor Ransomware schützen kann. Hier wurde zunächst auf präventive Möglichkeiten eingegangen.

Vorbeugend ist es wichtig eine Antiviren-Software auf dem Gerät installiert zu haben. Dies allein reicht aber längst nicht aus, vielmehr ist es sehr bedeutsam, dass man sensibel mit eingehenden E-Mails umgeht und diese stets überprüft. Darin enthaltene Links, Anhänge oder Dokumente können das Gerät im Folgenden befallen. Außerdem muss die Software des Geräts stets aktuell gehalten werden und Updates eingespielt werden. Daten sollten zusätzlich auch auf externen Datenträgern gespeichert werden.

Es stehen aber auch reaktiv einige Maßnahmen zur Verfügung, welche der Referent ebenfalls noch erläuterte. So empfiehlt er, die geforderte Geldsumme nicht zu bezahlen und sich stattdessen an die Polizei zu wenden. Die Daten können in manchen Fällen wiederhergestellt werden, hier ist es wichtig sich Informationen darüber zu beschaffen. Auch ein Backup kann in einem solchen Fall helfen.

Zusammenfassend kann man sagen, dass Ransomware in aktuellen Zeiten ein großes Problem darstellt. Jedoch stehen einige Schutzmaßnahmen zur Verfügung, denen man sich bewusst sein muss. Prävention ist dabei, wie in vielen Bereichen, wichtiger als Reaktion.

9. Veranstaltung: **„Sicherheitstests in der Entwicklung digitaler Produkte“** (07.12.2021) mit Prof. Dr. Lothar Braun, Hochschule Augsburg

Der Vortrag behandelte schwerpunktmäßig Schwachstellen und Sicherheitsprobleme, die bei digitalen Produkten auftreten können. Es wurde aufgezeigt, wie IT- Sicherheit erreicht werden kann. Der Referent stellte dazu einige Testmöglichkeiten aus seiner unmittelbaren Praxis vor.

Schwachstellen machen digitale Systeme verwundbar. So ist es unbefugten Personen in der Folge möglich, vertrauliche Daten zu lesen, diese zu verändern oder die Verfügbarkeit der Daten auf dem System einzuschränken. Schwachstellen sollten im Idealfall bereits im Vorhinein präventiv vermieden werden, sodass die Software und die darauf enthaltenen Daten erst gar nicht einer möglichen Manipulation und einem möglichen Missbrauch ausgesetzt sind.

Dies kann aber nur gelingen, wenn IT-Sicherheit über den gesamten Entwicklungsprozess eines digitalen Produkts, beziehungsweise einer Software, garantiert ist. Dabei spielen sowohl Risiko- und Bedrohungsanalysen, als auch verschiedene Tests eine wichtige Rolle. Auf die verschiedenen Testmöglichkeiten ging der Referent im Rahmen seines Vortrags näher ein.

Hier kommen grundsätzlich zwei verschiedene Testmöglichkeiten zur Anwendung. Auf der einen Seite existieren die Analysen des Quellcodes, des sogenannten Bauplans eines digitalen Produkts, und auf der anderen Seite gibt es die Analysen des finalen und fertigen Produkts. Beide Gruppen können dann wiederum in manuelle und automatische Tests unterschieden werden. Als Beispiel für manuelle Tests wurden sogenannte „Penetration Tests“ erläutert. Hier nimmt der Tester die Rolle des Angreifers ein. Ein Beispiel für einen automatischen Test stellt das sogenannte „Fuzzing“ dar. Hier werden falsche Eingabedaten erzeugt und es wird dann analysiert, wie das System damit umgeht und ob es möglicherweise abstürzt. Der Referent zeigte

anschaulich anhand von praxisnahen Beispielen, wie solche Tests durchgeführt werden können.

Der Vortrag verdeutlichte, wie wichtig es ist Schwachstellen und Sicherheitsprobleme während des gesamten Entwicklungsprozesses eines digitalen Produktes zu identifizieren und zu erkennen. Verschiedene Sicherheitstests helfen dabei und ermöglichen so eine hohe Sicherheit für den Nutzer des Systems vor Angriffen. Es ist empfehlenswert, die IT- Sicherheit in den Software Development Lifecycle zu integrieren.

10. Veranstaltung: **„Digitale Helfer – diese Programme sollte jede Firma kennen“** (19.01.2022) mit Manuel Schuster, Werbeagentur Schuster, Wirtschaftsjunioren & Thomas Hoch, Datenschutzbeauftragter

Es wurde zunächst durch die beiden Referenten erläutert, welche Vorteile digitale Helfer für die Nutzer mit sich bringen. Neben einer Verbesserung des gesamten Arbeitsflusses, das wiederum zu einer Zeitersparnis führt, können Papierberge abgeschafft werden. Ein weiterer positiver Effekt ist der bessere Schutz von Daten sowie die genaue Definition von Zuständigkeiten. Neben Textbausteinen wurden Passwortmanager sowie digitale Dokumentenablagen und Dokumenten Management Systeme (DMS) exemplarisch für die potenziellen Anwender mit ihren Vorteilen und Nachteilen vorgestellt.

Durch eine Sammlung vorbereiteter Texte können insbesondere bei sich wiederholenden Texten und Konversationen Zeit und Fehler gespart werden. Es gibt verschiedene Programme, wie etwa Phrase Express, die den Anwender hier unterstützen können.

Entscheidet man sich für die Nutzung eines sogenannten Passwortmanagers, welches Passwörter und Geheimzahlen verschlüsselt verwalten kann und auch Passwörter speichern sowie neu generieren kann, bestehen auch hier einige Vorteile. Zum einen wird auf diese Weise verhindert, dass man bei sämtlichen Anwendungen dasselbe Passwort verwendet, wodurch die Sicherheit deutlich gesteigert wird. Ein sicheres Passwort ist das A und O, um die persönlichen sensiblen Daten zu schützen. Zudem kann mit Hilfe des Passwortmanagers der Aufwand von Passwortgenerierungen sowie der Verwaltung der gesamten Passwörter einiger Aufwand eingespart werden. Im

Vortrag wurden auf die unterschiedlichen Bedürfnisse der verschiedenen Nutzer eigegangen und Themen wie Sicherheit und Verschlüsselung erläutert.

Zum Thema der digitalen Dokumentenablage wurden verschiedene Anwendungen wie beispielsweise Dropbox genannt und vorgestellt. Auch allgemeine Tools, die die Arbeit mit Dokumenten am Computer erleichtern, wie etwa 7- Zip oder Snipping Tool wurden in ihrer Funktion erläutert. Zu guter Letzt wurde ein Überblick über Sicherheitssoftware gegeben und deren Vorteile beleuchtet.

11. Veranstaltung: **„Alles Wolke oder heiße Luft? Immer Zugriff auf Ihre Cloud und mobile Sicherheit für Firmen“** (16.02.2022) mit Manuel Schuster, Werbeagentur Schuster

Die Veranstaltung drehte sich Rund um das Thema „Cloud“. Nach einer kurzen Vorstellung verschiedener Cloud – Anbieter erfolgte eine umfassende Erklärung, was eine Cloud und wie die Funktionsweise ist. Es wurden durch den Referenten verschiedene Cloud- Dienste und die entstehenden Kosten bei deren Nutzung für den Verbraucher aufgezeigt. Bei der Auswahl des Anbieters ist es wichtig, den Speicherort in Hinblick auf die DSGVO zu berücksichtigen. Neben Flexibilität, die durch die Nutzung einer Cloud entsteht, können einfach sowohl Rechner- als auch Speicherleistungen durch den Nutzer ausgelagert werden. Zudem kann die Speichergröße variiert werden. Da durch die Funktionsweise einer Cloud die Daten auf einem oder auch mehreren entfernten Server gespeichert werden, führt es durch die entstehenden Kopien der Daten zu einer höheren Datensicherheit. Bezüglich des Datenschutzes gilt es zu beachten, dass in verschiedenen Ländern verschiedene Datenschutzregeln gelten, so ist beispielsweise in Deutschland die Sicherheit der Daten besonders wichtig und der Zugriff auf die Daten klar geregelt, allerdings wird das in anderen Ländern anders gehandhabt. Vor dem Hochladen in die Cloud sollten Daten auf der Festplatte verschlüsselt werden. Bei besonders wichtigen Daten wird empfohlen, die Daten zusätzlich beispielsweise auf einer externen Festplatte oder einem USB Stick zu speichern. Eine regelmäßige Funktionsüberprüfung bei derartigen Speichermedien ist wichtig.

12. Veranstaltung: **„Datenschutz und Datensicherheit für mittelständische Unternehmen**“ (16.03.2022) mit Thomas Hoch, Datenschutzbeauftragter & Manuel Schuster, Werbeagentur Schuster

Zu Beginn der Veranstaltung wurden die Begrifflichkeiten Datenschutz und Datensicherheit definiert, sowie deren Unterschiede verdeutlicht. Während erster personenbezogene Daten schützt, bezieht sich zweiter auf einen generellen Schutz von Daten. Daraus lässt sich ableiten, dass für Datenschutz eine Datensicherheit notwendig ist.

Nach Klärung der Begrifflichkeiten wurde die Datenschutzgrundverordnung (DSGVO), welche seit dem 25. Mai 2018 in der EU aktiv ist, erklärt. Die DSGVO regelt die Verarbeitung personenbezogener Daten, zum einen zum Schutz von personenbezogenen Daten innerhalb der EU, zum anderen zum freien Datenverkehr innerhalb des europäischen Binnenmarktes. Personenbezogene Daten sind grundsätzlich Informationen, die Rückschlüsse auf die Identität einer Person schließen lassen, wie etwa dem Namen, der Adresse, der Emailadresse, Standortdaten etc. Personenbezogene Daten lassen sich in verschiedene Kategorien unterteilen, wie etwa in Gesundheitsdaten, politische Meinungen, religiöse Zugehörigkeiten usw.

Im weiteren Verlauf wurden Szenarien erläutert, wann Datenverarbeitung der verschiedenen Kategorien zulässig ist und welcher Datenschutz für Beschäftigte besteht (§ 26 BDSG (neu) gilt hier begleitend zur DSGVO).

Als besonders relevante Absätze aus der DSGVO für Datenschutzmanagement sind Art 5 DSGVO, Art 6 DSGVO, Art 28 DSGVO, Art 30 DSGVO, Art 32 DSGVO, Art 12-23 DSGVO zu nennen.

Datenverarbeitung ist komplex und besteht aus mehreren Komponenten, nämlich dem Erheben, Speichern, Ändern, Nutzen, Übermitteln, Verknüpfen und Löschen.

Insgesamt wurde nach dieser Einleitung tiefer in wesentliche Datenschutzvorschriften, die ePrivacy-Verordnung/TTDSG (Telekommunikations-Telemedien-Datenschutzgesetz) eingestiegen.

Es gilt zu beachten, dass Verstöße gegen die DSGVO zu rechtlichen Folgen wie beispielsweise Geldbußen oder Recht auf Schadensersatz führen kann.

Um eine DSGVO konforme Website zu gestalten, ist neben der Datenschutzerklärung und einem Cookie-Hinweis auch eine https- Verschlüsselung notwendig. Darüber hinaus gilt es Kontaktformulare, aber auch Newsletter oder Social Media Plugins entsprechend zu gestalten.

Weiterführende Hilfen sind etwa die Stiftung Datenschutz, eRecht24 oder auch die DGD. Insbesondere zu nennen sind Datenschutzbeauftragte, die einen mit fachlicher Expertise unterstützen können.

Zum Thema Datensicherheit wurde explizit auf Maßnahmen zum Schutz vor Hackern und Trojanern hingewiesen. Ganz konkret genannt wurde beispielsweise, dass sichere Passwörter notwendig sind, sowie E-Mail Anhänge von Fremden nicht geöffnet werden sollten. Auch die Installation von Anti-Viren Software sowie das regelmäßige Durchführen von Updates sind wichtig. Zudem sind Daten in einer Cloud sicher aufbewahrt, da die Daten extern abgesichert sind und so nicht durch äußere Einflüsse wie Brände, Diebstahl oder einen defekten PC gefährdet sind.

13. Veranstaltung: **„Die menschliche Firewall und ihre Löcher“** (16.05.2022) mit Cem Karakaya, blackstone432

Die Veranstaltung thematisierte zunächst die Widersprüche, die „der Mensch“ durch sein Handeln verursacht, wie etwa das Akzeptieren ungelesener Datenschutzbedingungen mit dem gleichzeitigen Ruf nach mehr Datenschutz oder aber auch die Partnerwahl nach Algorithmus. Der Mensch begibt sich in Gefahren, zum Teil durch Unwissenheit, zum Teil durch Unüberlegtheit und Dummheit. Der Blick auf ein Display ist häufiger als der Blick in die Augen derer, die „dem Menschen“ wichtig sind. Durch Corona wurde den Cyberkriminellen eine neue Chance an Möglichkeiten erleichtert, da sich viele Aspekte des täglichen Lebens ins Netz verlagert wurden und hierbei nicht immer achtsam umgegangen wird, etwa bei Gerätesicherheit im Allgemeinen, Kalendereinträgen, Phishingmails aber auch den Gästelisten im Restaurant mit unbedachter Angabe von Mailadressen, die für viele Personen einsehbar waren. Seit Corona ist die Internetkriminalität deshalb um 80% gestiegen, es gab einen Anstieg um 1200% bei Phishing Emails. Anhand realistischer Beispiele wurde den Teilnehmenden vom Referenten einige Vorgehen erläutert und aufgezeigt. Begonnen wurde mit Phishing und verschlüsselten Daten. Danach erfolgte eine

Erläuterung von Call-ID Spoofing, und dem angeblichen Support, der den Nutzer anruft, um an Daten zu gelangen. Hier ist auch die CEO- Masche zu nennen, die in der Anwendung sehr ähnlich funktioniert. Zusätzlich warnte er die Teilnehmenden, persönliche Daten am Telefon weiterzugeben, insbesondere dann, wenn man von einer anderen Nummer angerufen wird. Ein weiterer Punkt, bei dem Vorsicht angebracht ist, sind Anzeigen, sowie Onlineshopping. Hier gilt es immer, im Rahmen des Realistischen zu bleiben und nicht unüberlegt zu handeln. Themen wie Deep Fake am Beispiel einer Rede von Barack Obama wurden aufgezeigt. Ein weiteres Problem stellt Geldwäsche mit Gutscheinen als Bezahlung dar. Darauffolgend wurde anhand einiger Beispiele digitale Erpressung erläutert und erklärt, wie Trojaner etwa via Pornoseiten verbreitet werden. Auch Love Scamming wurde hier genannt. Als vorletztes Beispiel erläuterte der Referent Influence – Marketing und Fake Followerzahlen. Der letzte, und einprägendste Punkt war die Spionage mit der Feststellung, dass Ihr digitales Ich mehr über Sie weiß, als Sie selbst über sich wissen.

Ebenfalls betont wurde, dass es sich bei dem Smartphone ebenfalls um einen Computer handelt und man deshalb entsprechend mit diesem umgehen sollte, also Kindern einen Zugang limitieren soll und eine geeignete Antivirensoftware auf dem Smartphone installieren sollte, nicht zuletzt aus dem Grund, dass Deutschland täglich auf Platz zwei bis drei der Top drei am häufigsten angegriffenen Länder der Welt liegt. Im Darknet liegen aktuell über 12,3 Milliarden Emailadressen, bei denen das Passwort einsehbar ist. Es empfiehlt sich aus Sicherheitsgründen auf einen Passwortmanager zurückzugreifen und sich nicht Passwörter selbst auszudenken oder im schlimmsten Fall überall das gleiche Passwort zu verwenden. Ein weiterer Tipp zur Erhöhung der Sicherheit ist die Verwendung eines VPNs.

Als Fazit resümierte der Referent, dass Datenschutz so nicht mehr existent ist und es keine Frage ist, ob man getroffen wird, sondern lediglich wann.

Als wichtige, weiterführende Links sind folgende Seiten genannt worden: www.bsi-fuer-buerger.de www.selbstdatenschutz.info www.klicksafe.de www.verbraucherzentrale-bayern.de www.polizei-beratung.de www.schau-hin.de sowie das Buch des Referenten „Die Cyber-Profis – Lassen Sie ihre Identität nicht unbeaufsichtigt“.

14. Veranstaltung**: „Identitätsdiebstahl, Social Engineering, Awareness/ Sensibilisierung der Mitarbeiter, Darknet, Wirtschaftsspionage“** (19.05.2022) mit Cem Karakaya, blackstone432

Die „Digitalisierungsinitiative für Mensch und Wirtschaft“ wurde mit der Veranstaltung „Identitätsdiebstahl, Social Engineering, Awareness / Sensibilisierung der Mitarbeiter, Darknet und Wirtschaftsspionage“ abgeschlossen. Es wurde zunächst danach gefragt, was eigentlich Datenschutz ist. Hierbei wurde zusammenfassend festgehalten, dass alle jenes privat ist, was nicht jeder wissen darf. Thematisch wurden hier einige interessante Aspekte aufgegriffen, wie etwa der Tatsache, dass die meisten Menschen hier heute freiwillig das größte Spionagegerät, das Smartphone, mit sich herumtragen. Er wies darauf hin, dass einem nur selten etwas geschenkt wird und es viel häufiger der Fall ist, dass man mit seinen persönlichen Daten bezahlt. Es wurde den Teilnehmenden deutlich erklärt, was unter Datenschutz und persönlichen Daten zu verstehen ist. Als Privat wurde all jenes einkategorisiert, was nicht öffentlich sein soll und nicht jeder wissen darf. Was passieren kann, wenn die persönlichen Daten missbraucht werden, zeigte der Referent anhand eines persönlichen Beispiels auf. Im Anschluss wurde anhand einer Vielzahl anschaulicher Beispiele erläutert, was im Falle eines Missbrauchs der persönlichen Daten passieren kann, wie etwa Telefonnummernmissbrauch, Emailmissbrauch etc. Daraufhin erfolgten Tipps und Tricks, wie man sich vor Datenmissbrauch bestmöglich schützen kann. Zum Thema Identitätsdiebstahl, also dem Missbrauch personenbezogener Daten durch Dritte, wurden die verschiedensten Möglichkeiten wie Phishing, Pharming, Spim oder auch Wardriving den Teilnehmern lebhaft erläutert und vorgeführt. Empfohlen wird beispielsweise ein Aktenvernichter, da nach wie vor Kriminelle Müll durchwühlen, um Daten zu sammeln Es wurden sämtliche Möglichkeiten genannt, bei denen Identitäten geklaut werden können und welche Folgen ein Identitätsdiebstahl für den Betroffenen mit sich bringt. Als besonders wichtig für die Teilnehmerinnen und Teilnehmer können die darauffolgenden Tipps zum Schutz vor Identitätsdiebstahl gesehen werden inkl. der Empfehlungen geeigneter Tools.

Das Thema Social Engineering, also zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, um persönliche oder vertrauliche Daten freizugeben, wurde in Anschluss genauestens erklärt und auf Gefahren, insbesondere im Unternehmen hingewiesen. Auch das damit in

Zusammenhang stehende Social Hacking wurde den Teilnehmern erläutert. Hierbei wurde betont, dass die größte Schwachstelle im Menschen bzw. dem Mitarbeiter steckt. Gefahren liegen bei Mitarbeitern, die z.B. gefundene USB Sticks in der Firma testen, oder in den Mitarbeitern selbst, die Geld von Kriminellen erhalten, um bestimmte Vorgänge, wie einen USB Stick mit Viren in die Firma einzuschleusen. Es ist wichtig, zu testen, ob die Backups, die man durchführt, auch funktionieren. Es folgt ein fließender Übergang zum Thema Wirtschaftsspionage. Hier wurden Schäden, Sicherheit und Organisation in Relation gesetzt und die größten Probleme von Unternehmen analysiert. Auch der Umgang nach einer Wirtschaftsspionage im Unternehmen wurde aufgezeigt und Adressen genannt, an die sich Betroffene wenden sollen. Danach folgte ein Exkurs in das Dark und Deep Web mit allen Risiken. 91 Prozent des Internets sind Deep net und Darknet, wobei viele der Seiten sehr unzuverlässig sind. Im Anschluss an Tipps, wie man sich vor Datenmissbrauch schützt, erläuterte er noch, welche Sicherheitsprogramme er selbst verwendet. Zusammenfassend ist festzuhalten, dass eine dauerhafte Sensibilisierung der Mitarbeiter und der Unternehmen im Allgemeinen notwendig ist, der private Bereich jedoch auch auf keinen Fall vergessen werden darf, insbesondere auch Minderjährige. Zudem empfiehlt es sich, etwas in Sicherheitssysteme zu finanzieren, um sich und seine Daten zu schützen.

Unter www.datenklau-hilfe.de kann man sich geeignete Informationen beschaffen.