Handwerkskammer der Pfalz

Mobile Anwendungen und IT-Sicherheit

Digitalisierungsberater im rheinland-pfälzischen Handwerk

Projektträger:

RheinlandPfalz

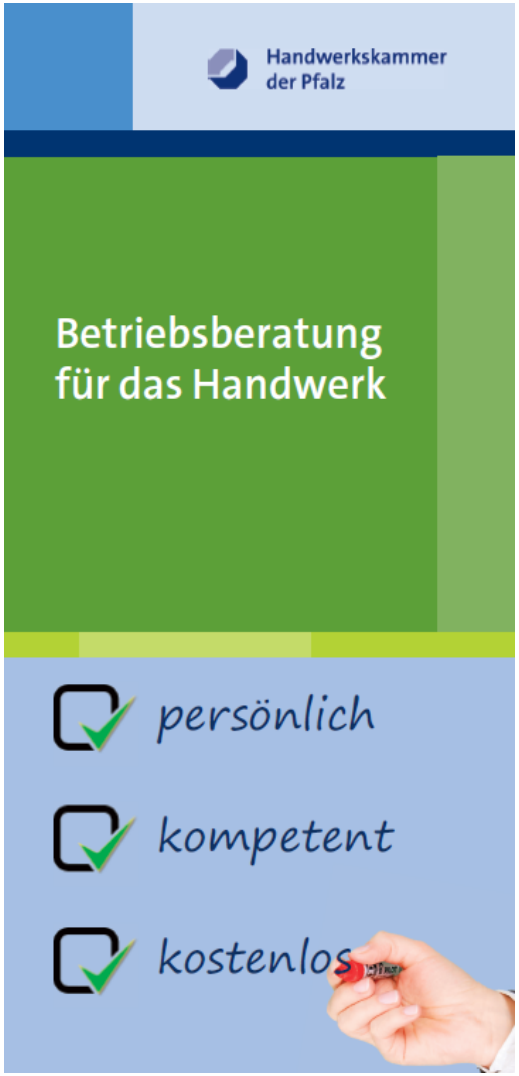
MINISTERIUM FÜR WIRTSCHAFT, VERKEHR, LANDWIRTSCHAFT UND WEINBAU

Digitalisierungsberatung

- ✓ Digitalisierungsberatung
- ✓ Webseiten-Check
- ✓ IT-Sicherheit
- ✓ Datenschutz
- ✓ Prozesse
- ✓ Förderprogramme

www.hwk-pfalz.de/digitalisierung

Beraterteam



Beratungsthemen

Kundenportal

Existenzgründung meistern

Betriebsnachfolge gestalten

Unternehmenswert ermitteln

Mitarbeiter gewinnen und langfristig binden

Innovationen entwickeln

Unternehmensleitbild entwickeln

Arbeitgeberattraktivität steigern

Betriebliche Gesundheitsförderung

Inklusion erfolgreich gestalten

Mediation zur Konfliktlösung

Unternehmenskrisen bewältigen

Betriebliche Kennzahlen analysieren

Neue Technologien einsetzen

Marketingstrategie entwickeln

Rentabilität planen und verbessern

Controlling durchführen

Investitionsvorhaben finanzieren

Förderprogramme berücksichtigen

Technische Normen erfüllen

Umweltschutzbestimmungen einhalten

Arbeitssicherheit erhöhen

Auslandsgeschäfte erfolgreich abwickeln

Was ist mobiles arbeiten?

Trend

Cloud-Computing

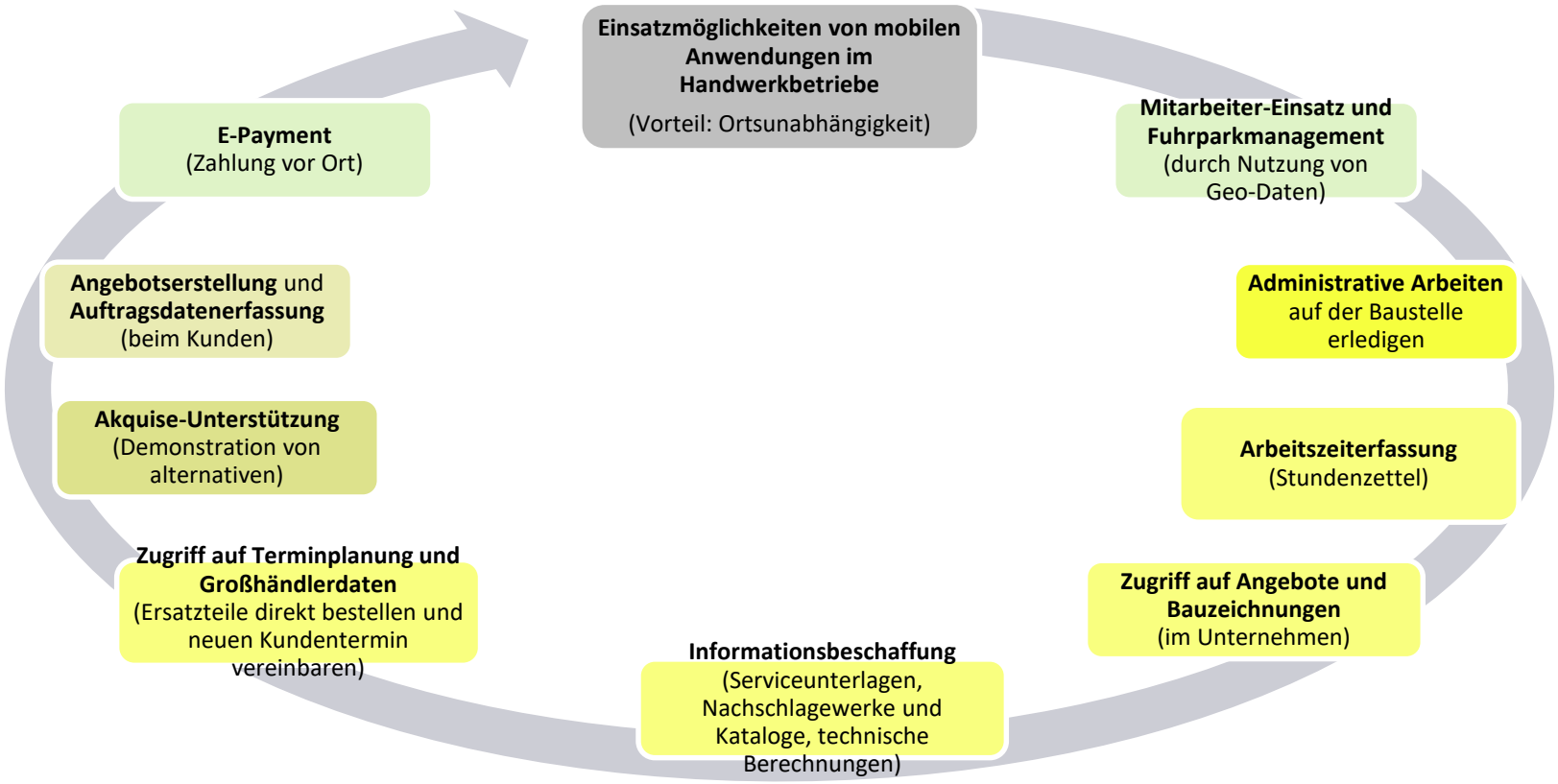
Quellen: www.expansys.de, www.letsgodigital.org, www.developers.google.com, www.flashusb.de, www.derspeicherplatz.de, www.onlinekosten.de, www.tapeonline.com, de.wikipedia.org, www.blogcdn.com, www.computerbild.de

Mobile Anwendungen

- Analoge Dokumente scannen z.B. Scanbot-App
  - Handbücher
  - Bedienungsanleitungen
- Betrieblicher Remote-Zugriff (Server, Netzwerk)
- Personal-Disposition/ Urlaubsanträge
- Projekte im cloudbasierten Speicher (work2gether)
- Digitale Kooperationsplattformen
- Online-Terminkalender
  - Online-Buchung & Bestätigung
  - Erinnerung
- Digitale Kundenkarte/login
- Buchhaltung
  - Rechnung per eMail und Upload (z.B. Datev)
- Rezeptions-Ipad: Digitaler Ordnerorganisation z.B. Evernote
- Online-Einkauf
  - Material- und Ersatzteile
- Flottenmanagement

Warum mobil arbeiten?

- ✓ Kooperation: gemeinsames Arbeiten über große Entfernungen
- ✓ Zugriff auf den aktuellen Datenbestand
- ✓ Zeit: schnellere Reaktion auf Kundenanfragen
- ✓ Kosten reduzieren: Einsparen von Mitarbeiter-Ressourcen
- ✓ Wettbewerbsvorteile: Unternehmen und Produkte beim Kunden multimedial präsentieren.


Einsatzmöglichkeiten von mobilen Anwendungen im Handwerkbetriebe
(Vorteil: Ortsunabhängigkeit)
Mitarbeiter-Einsatz und Fuhrparkmanagement (durch Nutzung von Geo-Daten)
Administrative Arbeiten auf der Baustelle erledigen
Arbeitszeiterfassung (Stundenzettel)
Zugriff auf Angebote und Bauzeichnungen (im Unternehmen)
Informationsbeschaffung (Serviceunterlagen, Nachschlagewerke und Kataloge, technische Berechnungen)
Zugriff auf Terminplanung und Großhändlerdaten (Ersatzteile direkt bestellen und neuen Kundentermin vereinbaren)
Akquise-Unterstützung (Demonstration von alternativen)
Angebotserstellung und Auftragsdatenerfassung (beim Kunden)
E-Payment (Zahlung vor Ort)

Digitalisierung der Unternehmensprozesse

- Ausführung analog

- Prozesse digital

Beispiel-Anwendungen (1/3)

Büro-Anwendungen

Email

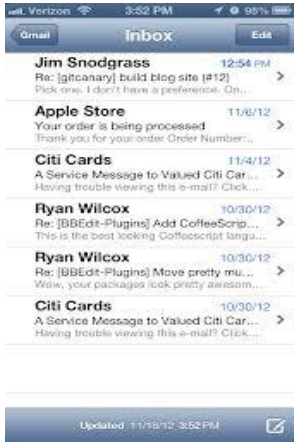
- als eigene App
  im Browser

PIM

- Termine, Kontakte,
  Aufgaben, Notizen, ...

Office

- Word, Excel, Powerpoint, ...
  ansehen und z.T. editieren

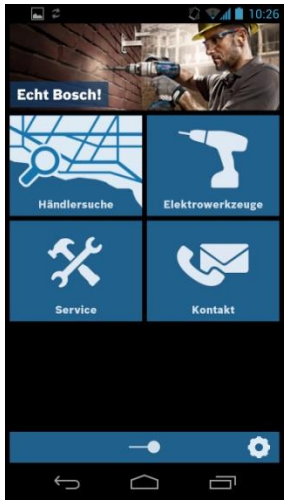


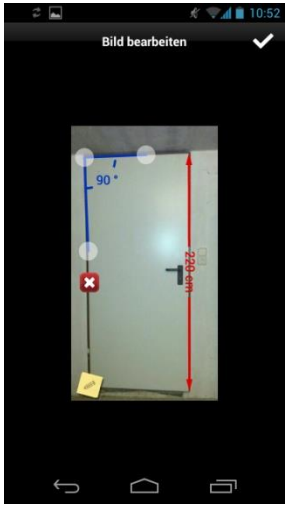
Beispiel-Anwendungen (3/3)

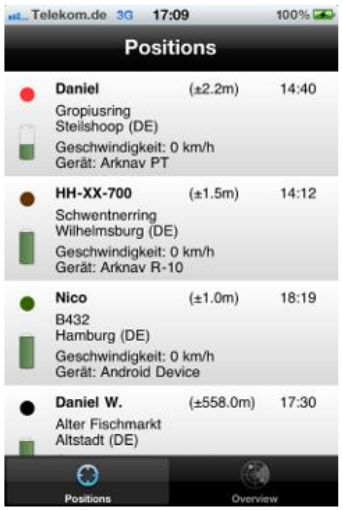
Handwerk-Anwendungen

Tools für Handwerker, z.B.

- Maßband, Wasserwaage oder Werkzeug-Infos
- Projekt-Dokumentation, Materiallisten
- Fahrtenbuch
- Rechnungen







Beispiel-Anwendungen (2/3)

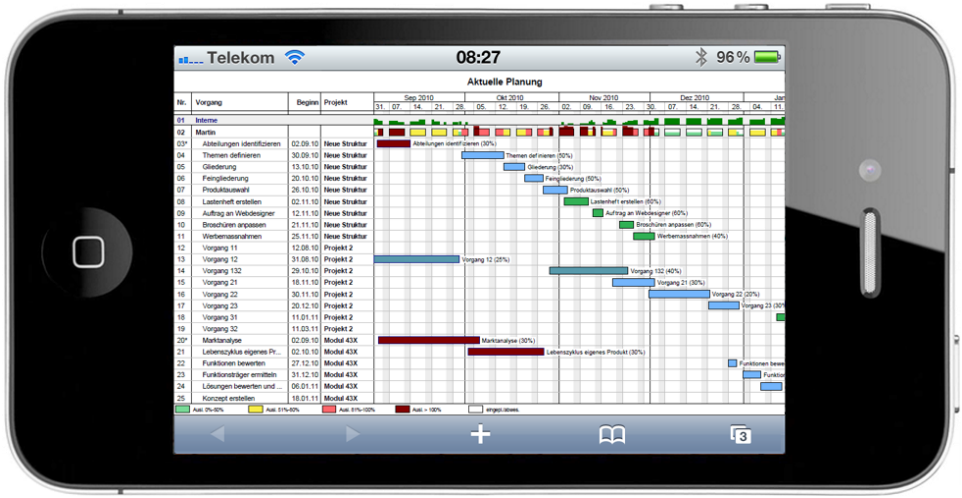
Büro-Anwendungen

Projekt- und Zeitmanagement

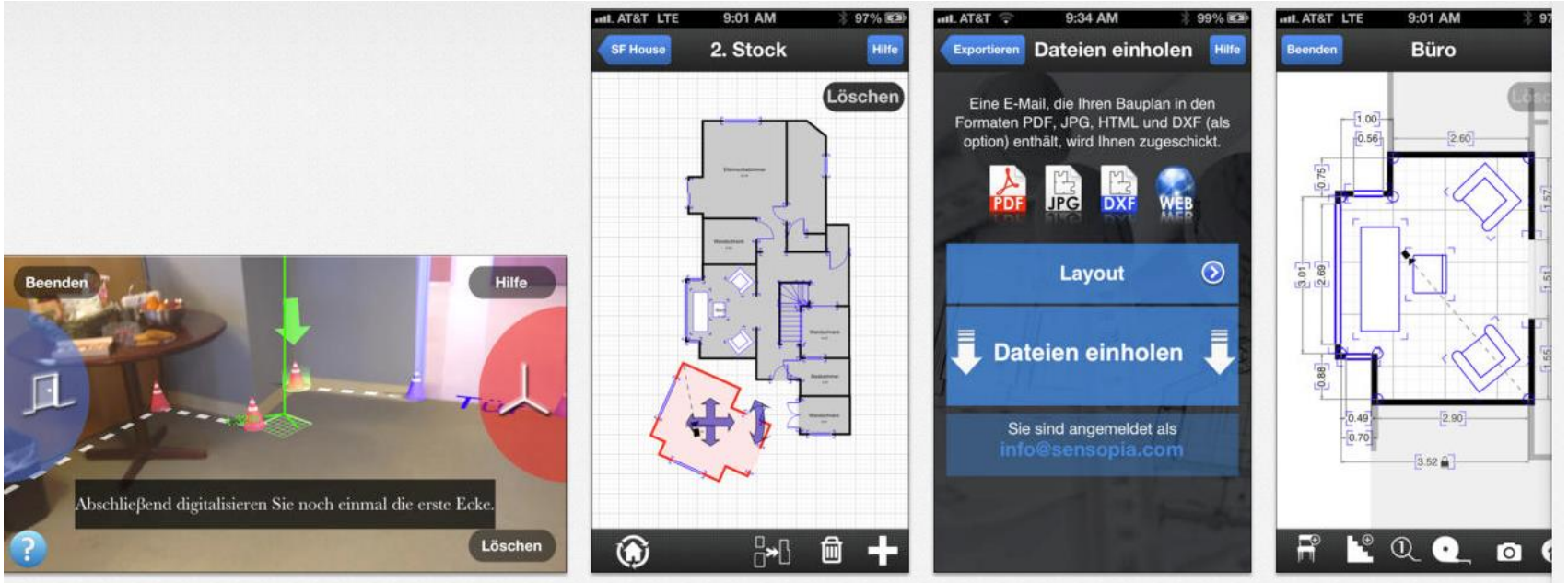
- persönliche Aufgaben
- Viewer für Projektpläne

Entfernter Zugriff auf

- Rechner im Betrieb
- z.T. besser für Tablets



Beispiel: MagicPlan
Anhand von Fotos lassen sich Pläne generieren und publizieren



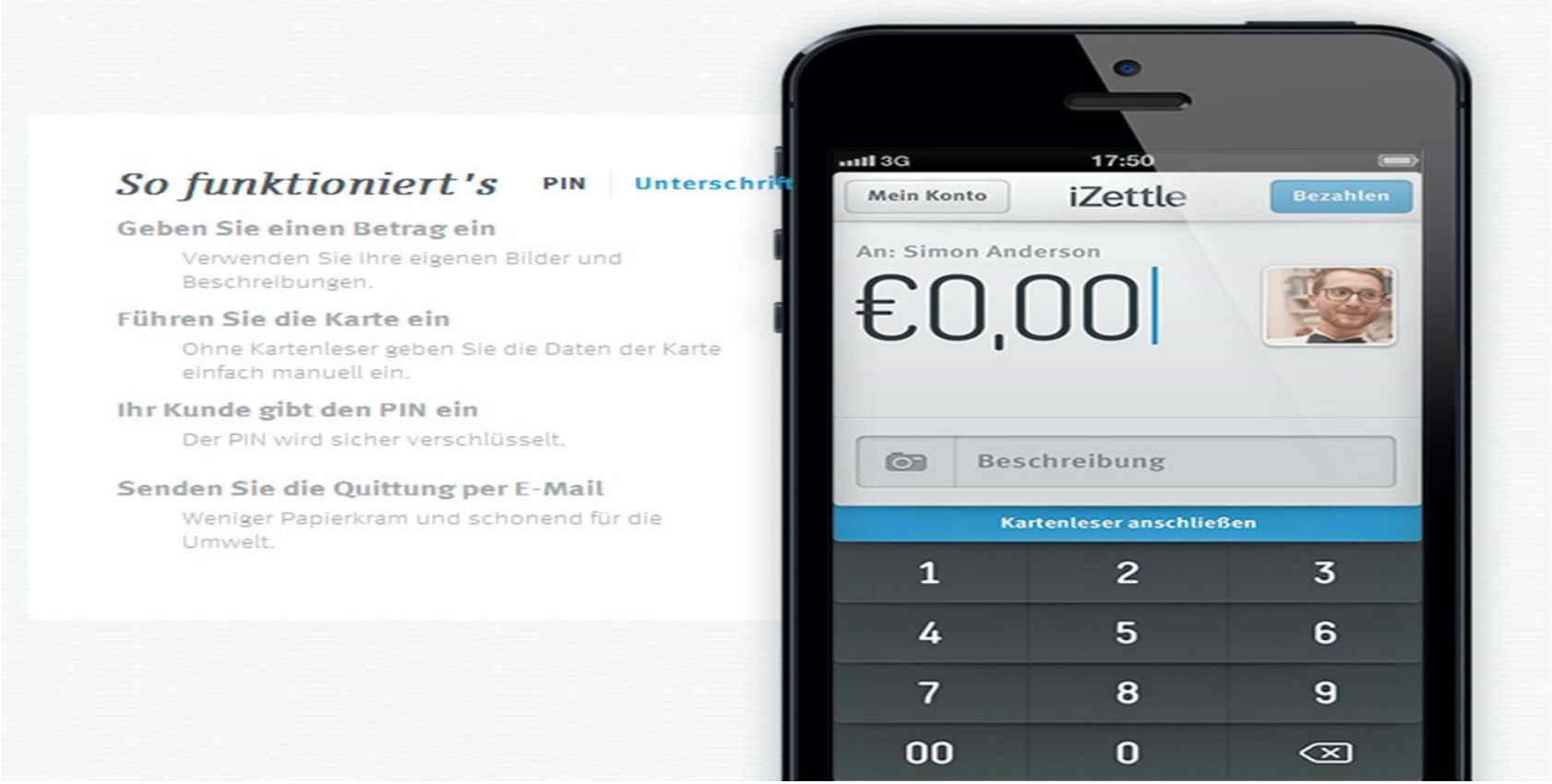
Beschreibung

MagicPlan ist die einzige Anwendung, die mithilfe einiger Fotos einen BAUPLAN EINES GEBÄUDES MISST, ZEICHNET UND VERÖFFENTLICHT. Mithilfe von MagicPlan sind Sie in der Lage INNERHALB WENIGER MINUTEN EINEN BAUPLAN ZU ERSTELLEN.

Beispiel E-Payment iZettle

- iZettle verfügt über EMV-Zertifizierung und erfüllt den Payment Card Industry Data Security Standard (PCI-DSS)
- Bei diesem Sicherheitsstandard werden sensible Daten weder auf dem mobilen Gerät noch auf dem Kartenleser abgelegt – der gesamte Datenverkehr erfolgt verschlüsselt.
- Der Service unterstützt EC-Karte sowie Kreditkarten von Visa und American Express

Beispiel E-Payment
iZettle



Smartphones – BYOD? COPE? CYOD?

- Link

- BYOD (Bring Your Own Device)
- Privates Gerät + dienstliche Nutzung
- Zugriff Dienstmails

- COPE (Corporate Owned, Personally Enabled)
- Dienstliches Gerät inkl. Privater Nutzung

- CYOD (Choose Your Own Device)
- Dienstliches Gerät inkl. Privater Nutzung
- Support von Mitarbeiter

Vereinbarung zur Gerätenutzung sowie der Trennung zwischen dienstlichen und privaten

Bring Your Own Device (BYOD)

Vorteil:

⊕ Anschaffungskosten

⊕ Geringer Aufwand

Nachteil:

⊖ Heterogene IT-Landschaft

⊖ TOMs schwierig umzusetzen

Zu beachten:

- Rechtsgrundlage des § 26 BDSG nicht ausreichend
- Von Mitarbeiter eine Einwilligung einholen (Zweck: private Rufnummer für dienstliche Zwecke wie Intranet, Aushang)

WhatsApp - Datenschutz Problematik Messenger

- WhatsApp
  - Vorteil: Versendung + Ende-zu-Ende-Verschlüsselung von Textnachrichten, Bildern, Videos und anderen Mediendaten
  - Datenschutz-Problem
    - Metadaten Nachrichten (USA)
    - Erhebung Kontaktdaten (Nutzer-Adressbuch)
    - Zwischenspeicherung 30 Tage bei nicht unverzüglich zugestellt Nachrichten
    - Facebook (Verwendung Profilname, Profilbild, Status, Handynummer (alle Messenger-Daten) der Facebook-Gruppe)
    - Auftragsverarbeitung (AVV) nicht vorhanden

Standortdaten wer mit wem kommuniziert, empirische Auswertungen (Werbezwecke)

WhatsApp – zu Beachten sowie ToDo

- Link

- Sicherheitslücke Gruppenchat -> Alternative: Signal, Threema, Wire, Telegram usw. Link Checkliste datenschutzkonforme Messenger
- Innerbetrieblichen Umfeld sichere Kommunikationswege prüfen (E-Mail, interner Chat) = Regelung Betriebsvereinbarung zur Nutzung von Internet und E-Mail aufstellen
- Verhaltens- und Leistungskontrollen Mitarbeiter (Statusanzeige zuletzt online, zur welcher Uhrzeit welche Nachricht), Statusfunktion deaktivieren (gerade online, Zeitpunkt Nachricht = Zeitpunkt nicht produktiv)
- Kunde
  - Hinweis Datenschutzbedenken
  - sicherer Kommunikationsweg anbieten (E-Mail PGP)

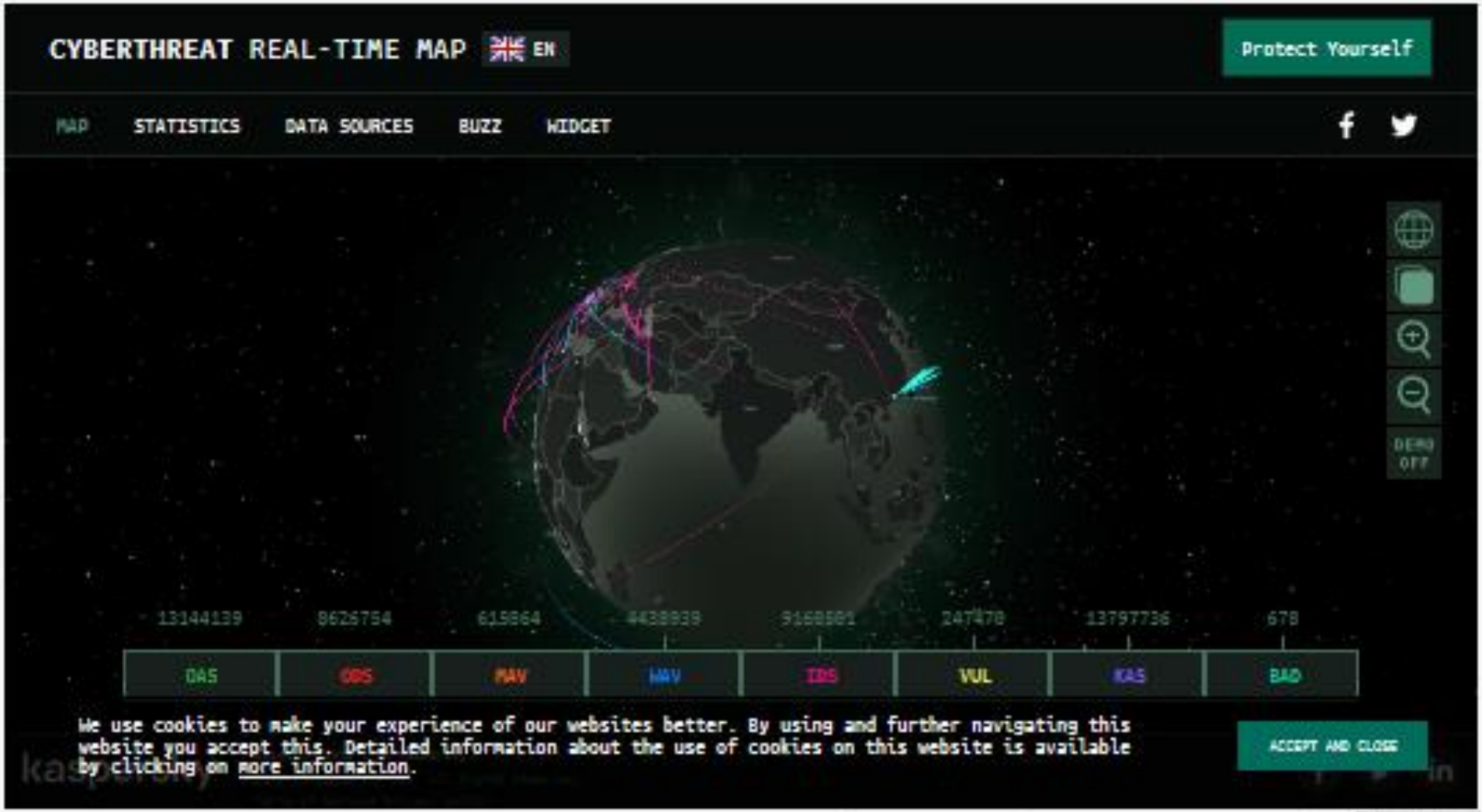
IT-Sicherheit

- Digitalisierung aber sicher!
- 20 zu 80 Prozent
- Unterschied gezielter Angriff oder Masse
- Alle Unternehmen, die in irgendeiner Form am Netz hängen, werden angegriffen.
- Unternehmensgrößer irrelevant
- Häufigkeit Cyberangriffe bei geringsten Widerstand (Kleinsbetriebe)

IT-Sicherheit – Hackerangriffe Nutzerdaten Historie

- **2013: Yahoo, 3 Mrd. Nutzer**
- **Sep 2018: Hotelkette Starford, Konzerntochter Hotelkonzern Marriott, halbe Milliarde Nutzerdaten (auch Kreditkarteninfo)**
- **Dez 2018: Quora, 100 Millionen Nutzerdaten (inkl. Inhalte)**
- **Januar 2019: Collection #1, 773 Millionen Online Konten**

IT-Sicherheit – Echtzeitkarte



Quelle: https://cybermap.kaspersky.com/

Webviewer Nutzungsbedingungen | Datenschutz und Cookies

Bearbeiten

IT-Sicherheit – Informationen

- Bestandsaufnahmen IT-Sicherheit (SICOM)
- IT-Sicherheit
  - Leitfäden
  - Broschüren
  - Handbücher
  - Checklisten
  - IT-Sicherheit im Handwerk
- Kostenfreie Kurse BSI (Link)

IT-Sicherheit – Netzwerk

- Router
  - Passwort-Werkseinstellung ändern (auch WLAN)
  - Herstellerupdates
  - Port Scan
  - Verschlüsselte Fernwartung (HTTPS)
- Backup
  - räumliche Trennung
  - Passwortgesichert oder verschlüsselt (z.B. Veracript)
  - Min. wöchentlich
  - Test/ Simulation
- Fernzugriff (z.B. VPN)

IT-Sicherheit – Basisschutz

- Aut. Updates
- ✓ Anti-Virus
- ✓ Firewall
- ✓ Betriebssysteme
- Anti-Virus
- ✓ Geräte-prüfung

- Betriebs-system
- ✓ Aut. Bildschirm-sperre
- ✓ Windows + L

- Dienstvereinbarung E-Mail und Internet am Arbeitsplatz

IT-Sicherheit – Sicher surfen

- Browser liefert Informationen an Web-Server:
  Name des Browsers, Betriebssystem, Referer, IP-Adresse, Session-Id, Cookies,

- **Installation von Browser-Updates**
- **Sicherheitseinstellungen des Browsers nutzen!**
- **Aktive Inhalte wie Java, Javscript und Active-X**

IT-Sicherheit – Tipps zu Online Banking

- Keine Testüberweisung machen
- Wenn Formular bereits vorausgefüllt ist (Felder Name, IBAN und Betrag sind befüllt) und man nur noch TAN eingeben muss sollte man aufpassen
- Bankinstitut sendet keine E-Mails zur Aufforderung der Dateneingabe

IT-Sicherheit – Passwortvergabe

- ✓ Ein E-Mail-Adresse und Passwort nie für mehrere Dienste nutzen
- ✓ Keine Fortlaufenden Passwörter, bspw. Kennwort1, Kennwort 2
- ✓ mind. 10 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- ✓ sinnfreie Zusammensetzung enthält weder den Namen, Vorname oder Geburtsdatum

IT-Sicherheit – Passwortaufbewahrung

- ✓ nicht auf einen Zettel schreiben und unter die Tastatur legen
- ✓ nicht unter den Deckel des Handys kleben
- ✓ nicht an den Monitor pinnen
- ✓ nicht in eine Textdatei am PC schreiben
- ✓ nicht im Browser speichern

IT-Sicherheit – Unternehmensinterne Passwortrichtlinien

- ✓ Sperrung des Nutzerkontos bei 3-5 Fehlversuchen
- ✓ Mindestanforderungen Passwort
- ✓ Regelmäßiger durch das System initiierter Passwortwechsel, bspw. nach 90 Tagen
- ✓ Unterbindung der Verwendung von alten Passwörtern (Passworthistorie; bspw. 5-10 Generationen).

IT-Sicherheit – Passwortveraltungsprogramme

- Ein Masterpasswort
- Beispielliste:
  - Keypass
  - 1Password
  - LastPass

IT-Sicherheit – Phising

- Problem
  - Missbrauch der Identität
- Vorgehen
  - Arbeitsgruppe Identitätsschutz
  - https://www.a-i3.org/beratungstelefon/

Datenschutz – Informationserteilung und Einwilligung – Newsletter

- Informationserteilung bei Datenerhebung
- Einverständniserklärung
  - Newsletter (Double-Opt-In)
    - Nutzer meldet sich zum Newsletter auf der Webseite an
    - Bestätigungsemail geht beim Kunden im Posteingang ein.
    - Kunde bestätigt ein zweites Mal das er den Newsletter erhalten will.
      - Bestätigung als Nachweis aufbewahren
    - Kunde erhält eine zweite Bestätigungsmail.
  - Veröffentlichung Fotos, Videos etc.

Datenschutz – Firmenwebseite

Muster
Generator

- Angaben zum Verantwortlichen
- Kontaktdaten Datenschutzbeauftragen (Optional)
- Arten der zu verarbeitenden Daten
- Zweck der Datenverarbeitung
- Rechtsgrundlage/Grundlage der Verarbeitung
- Speicherfrist
- Rechtauskunft
- Datenweitergabe an Dritte
- Umstände der Bereitstellung der Daten – gesetzliche oder vertragliche Vorschriften
- automatisierten Entscheidungsfindung

Datenschutz – Firmenwebseite – Tracking

- HTTPS
- Cookies
- Opt-Out Google Analytics
- GPS-Koordinaten
- www.siwecos.de

Disconnect

Shodan

GHOSTERY®

- Hinweis: DSGVO gibt keine technischen Standards vor!

3. Dokumentationspflicht – Verzeichnis der Verarbeitungstätigkeiten

Link Verzeichnis der Verarbeitungstätigkeiten

Muster- Verzeichnis von Verarbeitungstätigkeiten

© Jürgen Schüler

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	technische/ organisatorische Maßnahmen
Personalverwaltung		25.05.2018	* Personaladministration * Personalführung * Personalbeschaffung	* Beschäftigte * Auszubildende * Bewerber	* Name, Geburtsdatum * Adresse * Kommunikationsdaten (Telefon, Handy, E-Mail-adresse) * Daten zur Arbeitsleistung * Leistungsbeurteilung * Lebenslauf und Bewerbungsunterlagen	* keiner	keine	* Beschäftigte: 60 Jahre * abgelehnte Bewerber: 6 Monate nach Abschluss des Bewerbungs-verfahrens	Siehe IT-Sicherheits-konzept
Lohnabrechnung **durch** * Steuerberater [weisungsgebunden] * Rechenzentren	 ADV ADV	25.05.2018	* Auszahlung der Löhne / Gehälter * Abfuhr Sozialabgaben und Steuern	* Beschäftigte * Auszubildende	* Name, Geburtsdatum * Adresse * Lohn-/Entgeltdaten * ggf. Religionszugehörigkeit * Bankverbindungsdaten * Sozialversicherungsdaten * Steuerdaten (Steuerklasse, Freibeträge ...) * Berufsgenossenschaftsangaben	* Kreditinstitute * Öffentliche Stellen, die Daten aufgrund gesetzlicher Vorschriften erhalten (z.B.Berufsgenossenschaften, Sozialversicherungsträger, Finanzbehörden)	keine	* 10 Jahre (Gesetzliche aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Zeiterfassung		25.05.2018	* Arbeitszeitverwaltung	* Beschäftigte * Auszubildende	* Zeitwirtschaftsdaten	* Personalverwaltung * Lohnabrechnung	keine	* 3 Jahre (nach Ausscheiden)	Siehe IT-Sicherheits-konzept + HTTPS-Verschlüsselung
Telekommunikationsanlage (VoIP, DECT)		25.05.2018	* Erfassung der Telefonkosten nach Abteilungen	* Beschäftigte * Auszubildende	* Rufnummer von Anrufendem und Angerufenem * Gesprächsdauer * Auflegende/r	* Personalverwaltung	keine	* 14 Monate	Siehe IT-Sicherheits-konzept
Mobile Geräte (Tablets, Smartphones...)		25.05.2018	* Kommunikation mit Kunden und Betrieb	* Kunde	* Kunden-Name * Kunden-Adresse * Kunden-Kommunikationsdaten	* Beschäftigte * Auszubildende	keine		Siehe IT-Sicherheits-konzept

Datenschutz – noch zu beachten

- Mitarbeiter-Datenschutz: Compliance: Mitarbeiter
- Datenschutzbeauftragter (DSB) nach Art. 37 DSGVO
  - >= 20 Personen (siehe Art. 38 BDSG-neu)
    - Interner
      - Fachliche Qualifikation (Fortbildung der HWK Pfalz)
      - Kein Interessenskonflikt vorhanden
- Checkliste Technisch-Organisatorische-Maßnahmen (TOM)
- Auftragsdatenverarbeitung Art. 28 DSGVO AVV-Muster

Weiterführende Informationen

Veranstaltungskalender

Weiterbildungsbroschüre

Vielen Dank für Ihre Aufmerksamkeit!

Handwerkskammer der Pfalz
Am Altenhof 15
67655 Kaiserslautern

Telefon: 0631 3677232
Fax: 0631 3677263
E-Mail: itabatschnik@hwk-pfalz.de