„Kopf hoch – statt kopflos“

Ich stelle mich kurz vor

- IT-Forensiker, IT mobil Forensiker, Pentester
- Experte für Lauschabwehr
- IoT und Digital-Hacking
- EDV-Sachverständiger
- externer Datenschutzbeauftragter (TÜV)
- Geschäftsführender Inhaber der bridge4IT®
- Unparteiisch, neutral, unabhängig

IT-Forensik – Sherlock Holmes der IT?

- Tatort sichern – auch digital
- Beweise sichern
- strategische und operationale Vorbereitung
- Datensammlung
- Untersuchung / Datenanalyse
- Dokumentation
- Präsentation

Security Regeln durchsetzen

Schwachstellen dürfen nicht ignoriert werden

Das Azubi-Phänomen:

- Auszubildende durchlaufen unter Umständen viele Abteilungen
- Jede Abteilung hat ihre eigenen Berechtigungen
- Am Ende verfügt eine einzelne Person über alle Teilberechtigungen aller Abteilungen!

Der unbeaufsichtigte Unternehmens-PC:

Durch Hilfsbereitschaft, Freundlichkeit und gesellschaftliche Muster verlässt man für kurze Zeit den eigenen Rechner Tür-Aufhalten, Paket annehmen, …

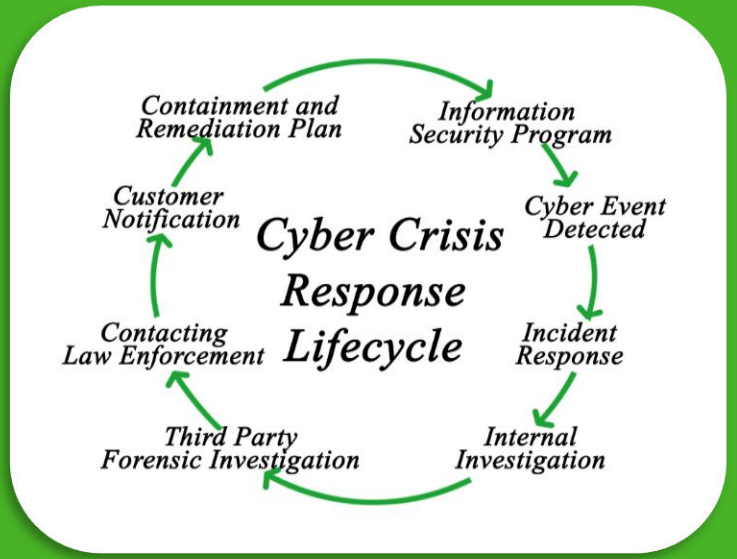
Kollege, Besucher, oder Eindringling?

Besucher müssen immer als solche erkennbar sein, denn:

- Niemand kennt jeden einzelnen Kollegen Besucher wird mit Kollegen verwechselt oder gibt sich als solcher aus
- Setzen Sie selbst auf Sicherheit, merkt der Besucher, dass er ebenfalls sicher ist

ERSTE HILFE

Hier sind Sie bestimmt gut vorbereitet!



Wie oft schon mussten Sie Ihre IT reanimieren?

Seien Sie vorbereitet – die beste Hilfe!

- ✓Festlegung Verfahren zu einzelnen IT-Prozessen (RedFolder)
- ✓Aktuellste Kenntnisse über Ihre IT
- ✓Notfallplan inkl. rechtlicher Rahmen / Ersthelferprinzip
- ✓Wo ist was? Dokumentationen aktuell halten und Kommunikationswege einbeziehen (RedFolder)
- ✓Checklisten zu Identifizierung des Angriffsziels (RedFolder)
- ✓Beweissicherung muss Teil des Notfallmanagement sein (RedFolder)
- ✓Backup-Tests und Zeiten der Wiederherstellung beachten (RedFolder)
- ✓Kontaktdaten der Hersteller und Dienstleister (RedFolder)

Chancen und Herausforderungen von digitalen Plattformen

- Plattformen stehen oft zwischen Anbietern und Kunden in jedem Land der Welt
- Bereitstellung digitaler Inhalte und müssen digital leben
- Maschinenbezogene Daten = personenbezogene Daten?
- Cloud Computing / KI / Machine Learning
- massive Anstieg von Bedrohungen auf Plattformen.
- Alle Plattformteilnehmer sind angreifbar
- Schnittstellen sind Ziel für Angreifer
- IoT Anbindungen oft unzureichend gesichert

Cloud Services unerlässlich, aber:

Warum die Cloud zur Digitalisierung nutzen?

- Kosten geteilt → Daten auch?
- Verfügbarkeit von Plattformen
- Compliance / Governance
- Dürfen die Daten in die Cloud?
- Verantwortung abgegeben?

Oder auch das Businessmodell

Angriffe sind sehr gezielter als jemals zuvor:

- HAFNIUM auf Port 443 und dann Türe von innen aufgemacht
- Versuch des Zugriffs auf Cloud-Logs
- RDP Protokoll
- HTTP Server
- FTP Server
- Schneller Datentransfer der Cloud-Leistung verhilft auch den Cyberkriminellen zum schnelleren Diebstahl
- Sprachassistenten

UND DER MENSCH!

Ziele der Angreifer:

- Kryptowährungs-Diebstahl
- Datendiebstahl
- Zahlungsmittel (Kreditkartendaten)
- Identitätsdiebstahl
- E-Commerce-Betrug

Cloud Security Posture Management

- **Verhindern von Cloud-Fehlkonfigurationen und Schwachstellen**

Cloud Access Security Broker

- **Authentisierung**

Cloud Workload Protection Platform

- **Micro Segmentierung**
- **Bare metal hypervisor**

Auswahl der geeigneten Plattform je Services ist wichtiger als je zuvor

MultiCloud

- Risiko für Plattformbetreiber und alle Teilnehmer
- Verteilt kann Kontrollverlust bedeuten
- Je mehr Systeme in der MultiCloud sind, umso angreifbarer sind diese
- Marktortprinzip im Datenschutz

IT-Forensik / Incident Response

- Verträge sind überwiegend mangelhaft gestaltet
- Verantwortung längst abgegeben
- Analyse von Plattformen erweist sich als Herausforderung (Wer liefert welche Infos?)

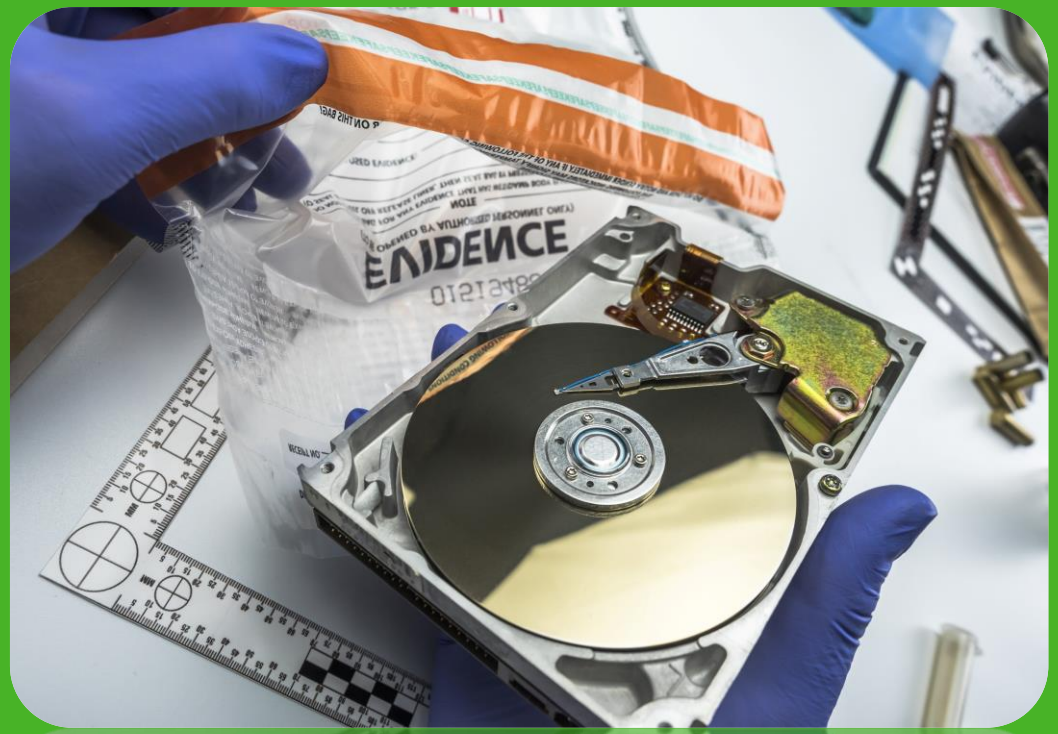
Alles oder nichts in der Cloud? Würden Sie beim Pokern ein All-in riskieren? Warum bei der IT?

- Ich mache mein Businessmodell und die Technik transparent für Wettbewerber
- Wieviel Sicherheit haben Sie beim All-In noch?
- Welches Risiko haben Sie?
- Was passiert, wenn Sie alles verlieren?
- Budget und Ressourcen für den Ernstfall?
- Die Cloud ist 24/7 – Sie auch?

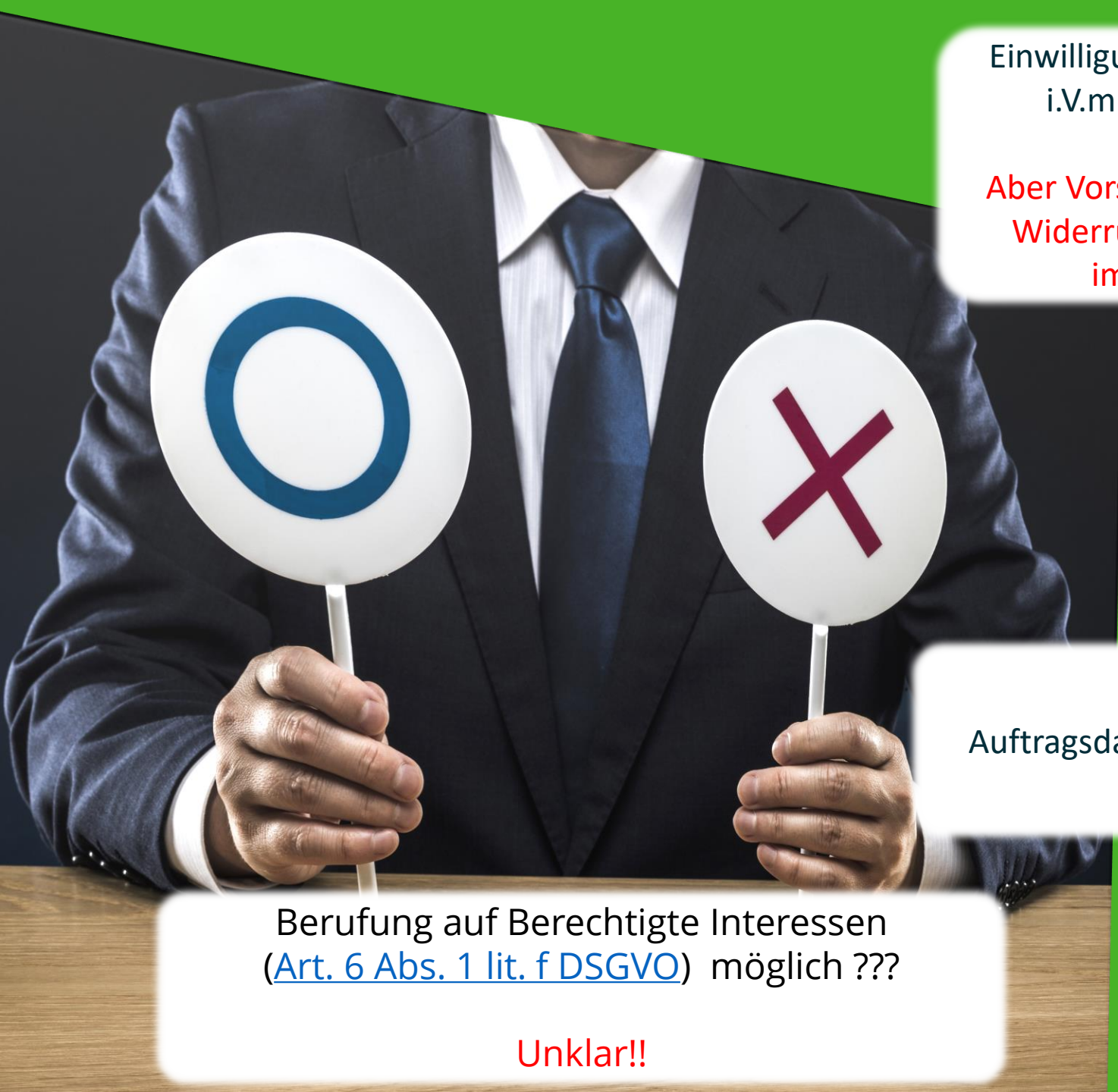
Backup & Recovery

- Datentransport
- Verschlüsselung
- Latenzen
- Volumen
- Zugriff / Zutritt
- Plan für die Zeit zwischen Ausfall und Recovery
- Personal
- Transport physikalisch

digital auf den
ausgefallenen Systemen!



- Notfall-Handbuch (teils PDF, teils Papier)
- Abfolge zur Lokalisierung des Angriffes (auch Cloud)
- Logging und erste Maßnahmen
- Rettung der Daten / Aufbau parallele IT
- Behördenkommunikation (Datenpanne / BSI)
- Risikobewertung
- Krisenkommunikation (Unternehmen und VIP)
- Ersthelfer-Training
- Kommunikationswege und Verantwortlichkeiten



Einwilligung gem. Art 7 DSGVO i.V.m. § 26 Abs. 2 BDSG

Aber Vorsicht! Informieren und Widerruf in die Einwilligung implementieren!

Standard-vertragsklauseln (SCC)

Durchführung des Arbeitsverhältnisses erforderlich, ist Rechtsgrundlage hierfür direkt § 26 Abs. 1 BDSG.

Auftragsdatenverarbeitung

Ausnahmen nach Art 49 zur Vertragserfüllung zwingend erforderliche Datenübermittlung ins Ausland

- Nicht anwendbar bei GPS -

Berufung auf Berechtigte Interessen (Art. 6 Abs. 1 lit. f DSGVO) möglich ???

Unklar!!

https://www.youtube.com/watch?v=mXMo0SbwHWw

You Are Wanted – erlebe Matthias Schweighöfer wie nie zuvor. Seine packende Amazon Original Serie ist jetzt bei Amazon Prime Video verfügbar. Als Lukas Franke kämpft Matthias Schweighöfer gegen unbekannte Täter, die seine persönlichen Daten hacken, sein komplettes Leben umschreiben und ihn und seine Familie bedrohen.

Es war einmal der 16. Juli 2020

Wer nimmt Daten mit?

Wer hat Zugriff auf Daten in der Cloud?

Wer hat die Berechtigung des Zutritt oder Zugriff?

Wer ist fachlich in der Lage den Datentresor zu bedienen?

Ist ein Passwortmanager im Einsatz?

Wer darf auf die Daten überhaupt rechtlich zugreifen?

In welchem Maße ist der Zugriff erlaubt?

- Daten zuerst Verschlüsseln und dann in die Cloud legen
- Endpoint-Security-Software mit verhaltensbasierter Erkennung
- Definition von Service-Leveln für Cloud Restore
- Auswahl, welcher Service für den Einsatz in der Cloud geeignet ist
- Bindung von Dienstleistern mit Notfall-Service-Verträgen
- definierte Reaktions- und Wiederherstellungszeiten aus der Cloud heraus
- Sicherung aller Daten die zum Erhalt des Betriebs erforderlich sind.
- Verschlüsselung der Kundendatensätze in allen führenden Systemen nach dem Stand der Technik (BSI-Standard)
- IT-Forensic-Readiness-Trainings, um IT-Personal auf mögliche Unterstützungsanforderungen vorzubereiten, die im Incident an den IT-Forensiker zu leisten sind.
- Bindung von finanziellem Budget für IT-Sicherheit und Ernstfall-Kapital
- Jede Software muss heterogen ausgelegt sein und portierfähig sein
- Sicherheitsupdates / Patches Hotfixes / Gleicher Stand onpremise und Cloud
- Passwort-Vorgabe und Richtlinien auch für die Cloud
- Einbeziehung der Sicherheitsmaßnahmen unabhängig der Betriebssysteme
- Das IT-Sicherheitskonzept muss auf alle Betriebssysteme angepasst und einheitlich sein
- BYOD ist zu untersagen
- Schutz von personenbezogenen Daten, Verfügbarkeit und Belastbarkeit von Systemen liegt in der Verantwortung des Cloudanbieters

Bitte stellen Sie Ihre Fragen direkt!

bridge4IT®
Volker Wassermann
Siemensstraße 18
D-47608 Geldern
Germany

+49 2831 395 909 50
vw@bridge4IT.de