VACE SECURITY

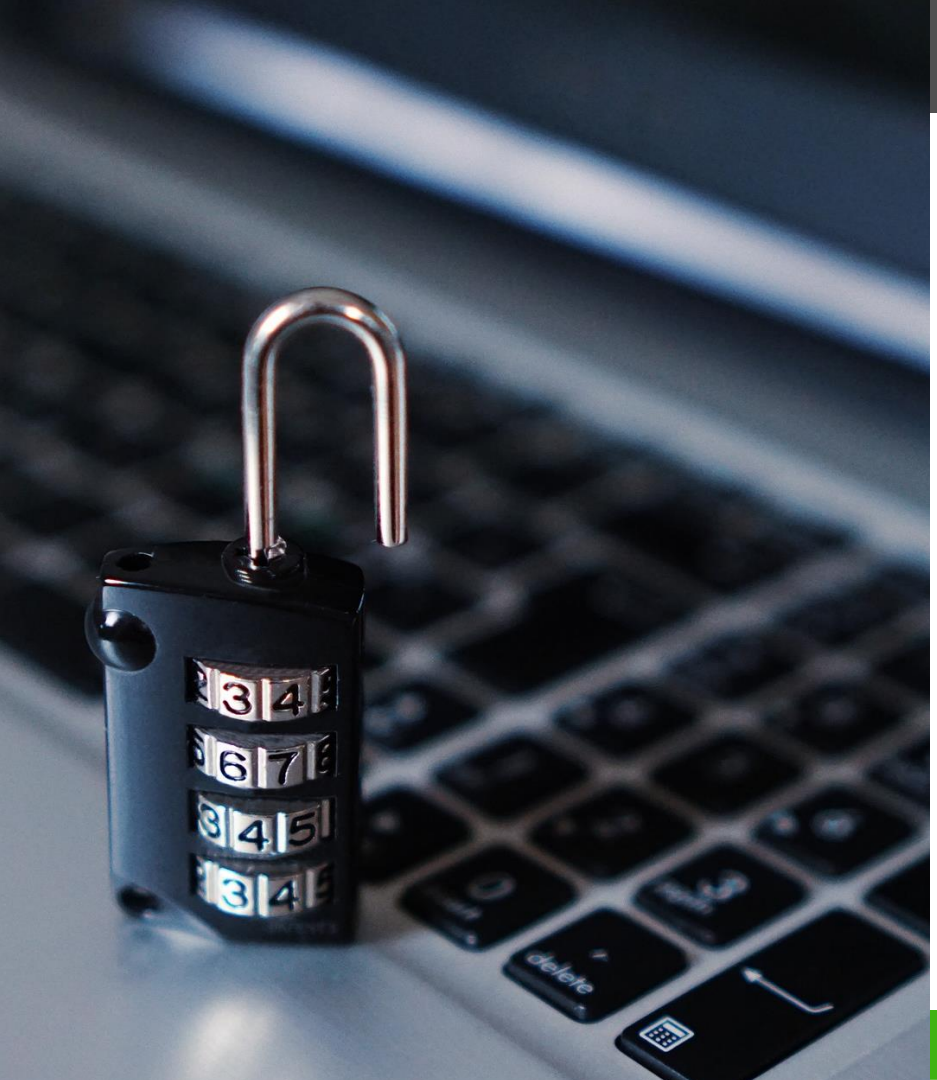
ÖGWT
IHR SERVICE-NETZWERK

EU-DSGVO & Hacking

Wie sicher sind Ihre Daten?

www.vace-sec.at

VACE Systemtechnik GmbH
business unit SECURITY
Linzer Straße 16e, 4221 Steyregg

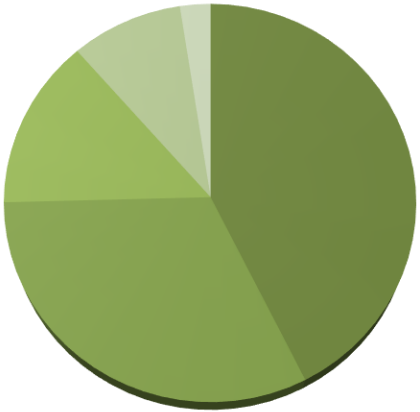


Aktuelles

- **31.08.2017: Herzschrittmacher**
  Herzschrittmacher sind auf Angriffe anfällig und die Konfiguration kann von unbefugten Personen manipuliert werden.
- **12. Mai 2017: WannaCry**
  Ransomware, die sich über öffentlich bekannte Schwachstellen in XP und anderen Windows Systemen verbreitet.
- **März 2017: Bulmor Industries**
  Spionage durch Hinweis des Mitbewerbs vereitelt.
- **August 2016: Leoni**
  Betrugsfall durch Phishing-Angriff – Summe ca. 40 Millionen Euro
- **Jänner 2016: FACC**
  Betrugsfall mit Schaden von ca. 50 Millionen Euro

Wer & Was: **Aktuelle Bedrohungen**

- Über 50% aller Unternehmen sind bereits betroffen
- Alle betroffenen Unternehmen nutzten Virenscanner, Firewalls sowie Passwortschutz
- Beliebteste Angriffsziele sind die Automobilindustrie, Chemie- und Pharma-Branche sowie Banken und Versicherungen



Quelle Bitkom.org 09.07.2015
Studie zu Wirtschaftsschutz und Cybercrime

Heartbleed, Ghost, Glibc

Fehler in breit verwendeten, als sicher eingeschätzten Technologien - siehe OpenSSL, Glibc

Öffentliche Einrichtungen

Cyberangriffe richten sich auch gegen öffentliche Einrichtungen. Alle IT Systeme können von Angriffen betroffen sein.

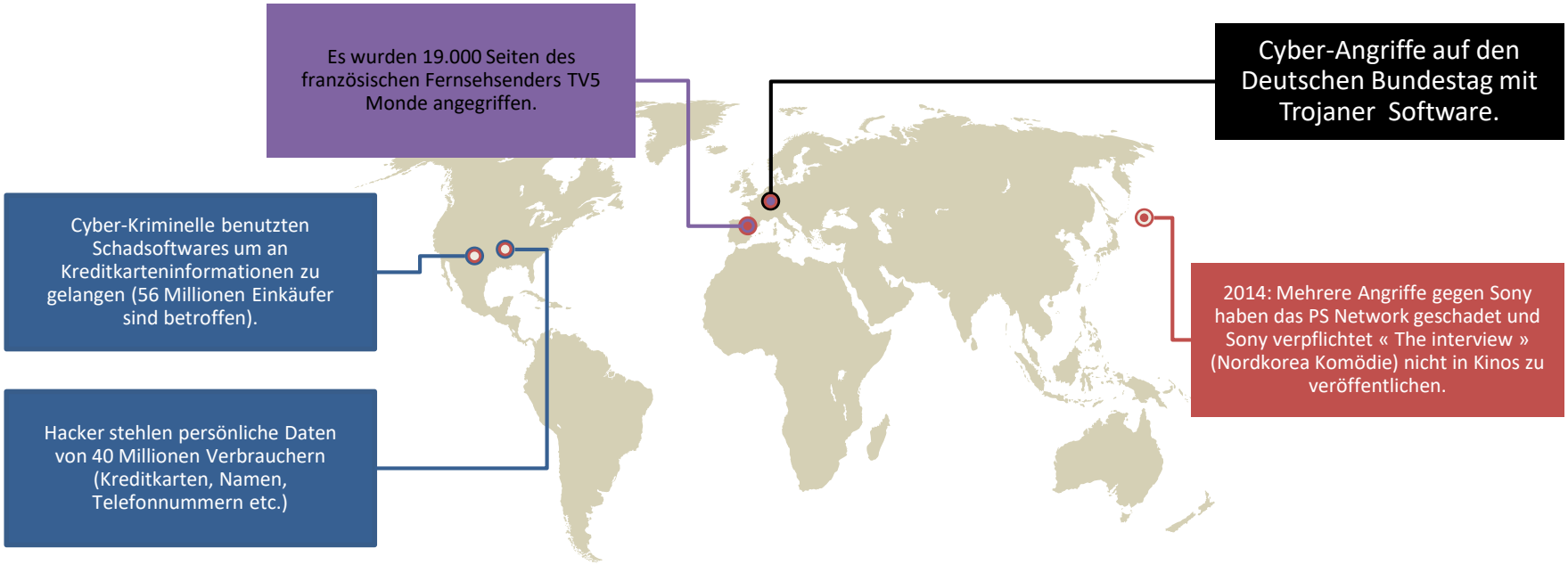
Whistleblower

Geheimdienste erspähen Kundendaten. Admins haben Zugriff auf fast alle Daten. In Europa laufen mindestens dreimal so viele Daten über verschlüsselte Verbindungen wie noch Anfang 2013.

KRITIS

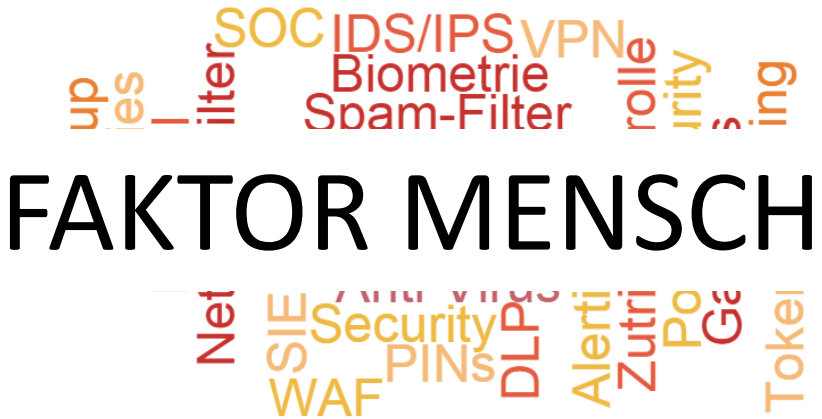
Wir sind mehr denn je von technischen Systemen abhängig. **Krit**ische **I**nfra**s**trukturen Strom, Trinkwasser, Informations- und Kommunikationstechnologie, Bankwesen, Treib- und Brennstoff, Verkehr, …
Die **NIS Richtlinie** für „**N**etz- und **I**nformations-**S**icherheit“ tritt zeitgleich zur EU-DSGVO im Mai 2018 in Kraft.

Wer & Was: **Aktuelle Bedrohungen**



Die Cyber-Kriminalitätsstatistik des Bundeskriminalamts zählt 64.426 Cyber-Angriffsvorfälle für das Jahr 2014 in Deutschland.

Vielseitigkeit der IT-Security


SOC
IDS/IPS
VPN
Biometrie
Spam-Filter
FAKTOR MENSCH
Security
PINs
WAF
DLP
Alerti
Zutri
Token

Bedrohungsszenarien - Beispiele

BEZEICHNUNG	ERKLÄRUNG
Hacking-Angriff	Unbefugte Personen nutzen Schwachstellen in der IT-Infrastruktur, um Daten missbräuchlich zu entwenden.
Phishing & CEO-Fraud	Mit Hilfe von gefälschten E-Mails wird versucht, Unternehmen und Privatpersonen zu bestimmen Handlungen, z.B.: Überweisung eines Geldbetrages, zu bewegen.
Social-Engineering	Eine unbefugte Person vor Ort oder am Telefon nutzt menschliche Eigenschaften, wie zum Beispiel Hilfsbereitschaft, um sich Zugang zu Informationen zu verschaffen.
Fehlkonfiguration	Nicht ausreichend sichere Konfigurationen von Systemen und Anwendungen eröffnet Sicherheitslücken im Unternehmen.
Fehlendes Bewusstsein	Nicht ausreichendes Training und mangelnde Bewusstseinsschaffung führt zum Nicht-Erkennen von verdächtigem Verhalten.
Unachtsamkeit	Der Alltagsstress und die steigende Geschwindigkeit der Gesellschaft führen zu schnelleren und somit unachtsameren Verhalten.

Rechtliche Rahmenbedingungen: EU-DSGVO

- **Grundrecht für EU Bürger** Die Europäische Union verankert den Schutz, **natürlicher Personen** betreffende, personenbezogene Daten auf **Grundrechtsebene**
- **EU-weites Datenschutzrecht** Die Verordnung ist der Versuch alle 28 bestehende nationale Gesetz zu vereinheitlichen – auf Grund der **Öffnungsklauseln** unzureichend
- **Sanktionen**
  - bis 10 Mio. € bzw. 2% des weltweiten Vorjahresumsatzes
    - Bei Verletzung technischer und organisatorischer Schutzmaßnahmen
    - Fehlender Nachweis der Verarbeitungstätigkeit, Datenschutz-Folgenabschätzung
  - bis 20 Mio. € bzw. 4% des weltweiten Vorjahresumsatzes
    - Verletzung der Rechtmäßigkeit, mangelnde oder nicht vorhandene Einwilligung
    - Verletzung der Rechte Betroffener
    - Drittlandübermittlung
    - Fehlende Zusammenarbeit mit der Aufsichtsbehörde

- **Beweislastumkehr**: der Verantwortliche muss die Rechtskonformität seiner Datenverarbeitung nachweisen.
- **Meldepflicht** bei Datenschutzvergehen, innerhalb von 72 Stunden an die Behörde und die Betroffenen.
- **Handlungsbedarf** – die Maßnahmen sollten bis zum **25. Mai 2018** bereits umgesetzt sein!

Datenschutz Grundverordnung EU-DSGVO

Wann dürfen personenbezogene Daten verarbeitet werden!

- Wenn von der betroffenen Person eine **Einwilligung** zur Verarbeitung vorliegt
  - Der **Text der Einwilligung** muss vom „Verantwortlichen“ zweifelsfrei nachgewiesen werden können
  - **Zustimmung** und **Widerruf** müssen in einfacher Sprache gleichermaßen präsent sein (Textgröße, Formulierung, Optik, …)
  - **Zweck** der Verarbeitung muss in klaren Worten dargelegt werden
  - **Datenminimierung** ist vorgeschrieben
  - Daten dürfen nur nach **Treu und Glauben** also zum eindeutigen Zweck der Erhebung, verarbeitet werden

- Zur Abwicklung eines **Vertrages**
  - **Kopplungsverbot:** es dürfen an die Erhebung der Daten keine weiteren Angebote/Verträge gekoppelt werden. Es gilt das Gebot der **Freiwilligkeit**.

- Zur Erfüllung **rechtlicher** Verpflichtungen
  - **Verträge**
  - Rechtliche **Aufbewahrungsfristen**

- Zur Wahrung berechtigter Interessen, öffentlicher Interessen bzw. Ausübung öffentlicher Gewalt

Grundsätze der Datenverarbeitung!

- Personenbezogene Daten dürfen nur **solange aufbewahrt** werden, wie es für den ursprünglichen Zweck, für welchen sie erhoben wurden, unbedingt erforderlich ist.
  - Sobald der Zweck erfüllt ist oder der Betroffene es wünscht, müssen die Daten **gelöscht** werden.

- Die Integrität und Vertraulichkeit der Daten muss am „Stand der Technik“ sowie mit entsprechenden organisatorischen Maßnahmen sichergestellt werden. Die Daten müssen vor
  - **unbefugter** oder **unrechtmäßiger** Verarbeitung
  - sowie vor unbeabsichtigtem **Verlust** oder **Schädigung** vom „Verantwortlichen“ geschützt werden

- **„Verantwortliche“** tragen die Verantwortung, unabhängig ob sie selbst oder externe Auftragsverarbeiter (Outsourcer, Cloud Service Provider und dgl.) ihre Daten verarbeiten.
  - Der „Verantwortliche“ muss jederzeit gegenüber betroffenen Personen sowie den Datenschutzbehörden die Rechtmäßigkeit und die Einhaltung der Vorschriften **nachweisen** können.

- Jeder Betroffene hat das Recht
  - eine **Bestätigung** darüber zu bekommen ob und welche Daten von ihm verarbeitet werden
  - eine **Kopie** seiner elektronisch verarbeiteten Daten in einem gängigen Format wie Bsp. XML, CSV, DOC, usw. zu verlangen
  - Er kann jederzeit seine **Einwilligung** zur Verarbeitung **widerrufen.**
  - Er kann die **Korrektur** seiner Daten verlangen.

Verzeichnis der Verarbeitungstätigkeiten & Dokumentationspflicht

Jeder „Verantwortliche“ führt ein Verzeichnis aller Verarbeitungstätigkeiten:

- Beschreibung der getroffenen **technischen Maßnahmen**
- Beschreibung der **organisatorischen Prozesse** zum Datenschutz
- **Name** und **Kontaktdaten** des Verantwortlichen
- **Kategorien** betroffener Personendaten und der Empfänger
- **Zweck** der Verarbeitung
- **Fristen** für die Löschung der Daten nach Kategorien
- Bei der Übermittlung personenbezogener Daten in ein **Drittland** müssen diese mit entsprechenden Garantien dokumentiert werden.

- **Dokumentationspflicht**
  - **Alle** Datenverarbeitungen mit personenbezogenen Daten sind zu dokumentieren.
  - Entsprechend der **Eintrittswahrscheinlichkeit** und der schwere der **Risiken** sind adäquate technische und organisatorische Maßnahmen für die rechtmäßige Verarbeitung zu setzen und zu dokumentieren.
  - Ergibt die Risikoabschätzung auf Grund von Technologien, Art oder Umfang ein **hohes Risiko** bei der Verarbeitung, ist vorab zwingend eine Folgenabschätzung zu machen.
  - Die korrekte Implementierung ist vom Verantwortlichen zu **überprüfen.**
  - Die Risikoabschätzungen und Dokumentationen sind **regelmäßig** zu prüfen und zu aktualisieren.
  - Dokumentation der Maßnahmen können von der Datenschutzbehörde **überprüft** werden!

Welche Daten dürfen nicht be- bzw. verarbeitet werden!

- Verbot der Bearbeitung **besonderer Kategorien**, dieses Verbot umfasst die Verarbeitung personenbezogener Daten, aus denen
  - die **rassische** und **ethnische** Herkunft
  - **politische** Gesinnung
  - **religiöse** oder **weltanschauliche** Überzeugung oder
  - die **Gewerkschaftszugehörigkeit**

  hervorgehen, sowie die Verarbeitung von
  - **genetischen** Daten
  - **biometrischen** Daten zur eindeutigen Identifizierung natürlicher Personen,
  - **Gesundheitsdaten** (Brillenträger, Diabetes/Kantine, …) oder
  - Daten zur **sexuellen** Orientierung.

- Ausnahmen für Verarbeitung besonderer Kategorien:
  - **ausdrückliche Einwilligung** bzw. lebenswichtige Interessen ohne Einwilligung
  - Erfordernisse aus dem **Arbeitsrecht**
  - wenn die Daten der betroffenen Person **selbst öffentlich gemacht** wurden
  - zur Geltendmachung von Rechtsansprüchen vor **Gericht**

Privacy by Design bzw. **Privacy by default**

- **Privacy by Design** bedeutet Datenschutzvorschriften bereits bei der Entwicklung neuer Applikationen/Prozesse/Technologien zu berücksichtigen
  - **Datensparsamkeit** nur jene Daten welche dem Zweck entsprechend erhoben wurden
  - **Löschfristen** automatische Löschung von Personendaten und Verifizierung ihrer Aktualität
  - **Datenkorrekturen** entsprechend dem Recht auf Richtigstellung
  - **Auskunftspflicht** Benachrichtigung welche personenbezogenen Daten sind gespeichert?

- **Privacy by default** bedeutet umfassender Schutz der Personendaten ohne Konfiguration
  - datenschutzfreundliche Voreinstellungen
  - **Opt-In**: Haken zur Einwilligung muss händisch gesetzt werden

BEDROHUNGEN

Phishing

ANGREIFER

Jeden Tag tauchen zahlreiche neue Formen von Schadsoftware im Internet auf

Trojaner & Würmer

WERDEN MIT INFIZIERTEN EMAILS VERSCHICKT

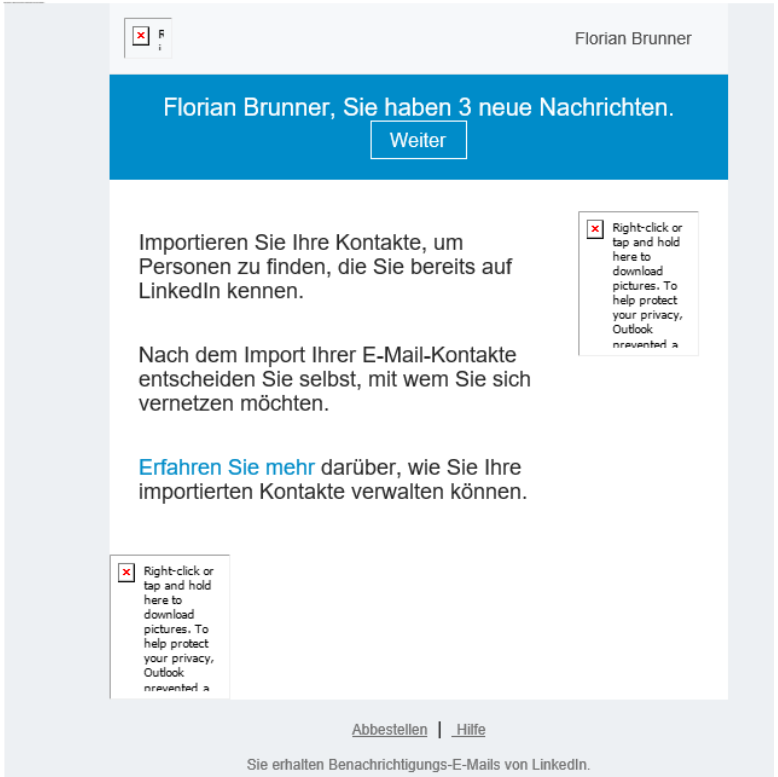
Können sensible Daten wie Passwörter, Bankinformationen oder personenbezogene Daten übertragen

OPFER

Malware setzt sich unbemerkt in Computersystemen fest oder schleicht sich während Downloads ein

Phishing – LinkedIn

From: LinkedIn [mailto:messages-noreply@linkedlin.de]
Sent: Donnerstag, 11. Mai 2017 12:13
To: florian.brunner@cybersecurityaustria.at
Subject: Florian Brunner, Sie haben 3 neue Nachrichten!



From: LinkedIn [mailto:messages-noreply@linkedlin.de]
Sent: Donnerstag, 11. Mai 2017 12:13
To: florian.brunner@cybersecurityaustria.at
Subject: Florian Brunner, Sie haben 3 neue Nachrichten!

ABHÖREN & SPIONAGE

Telefongespräche via Internet

TISCHLEREI HOLZ

Die Tischlerei diskutiert schützenswerte Informationen.

ANGREIFER

Ein zu erwartender Verlust wird am VoIP-Telefon diskutiert.

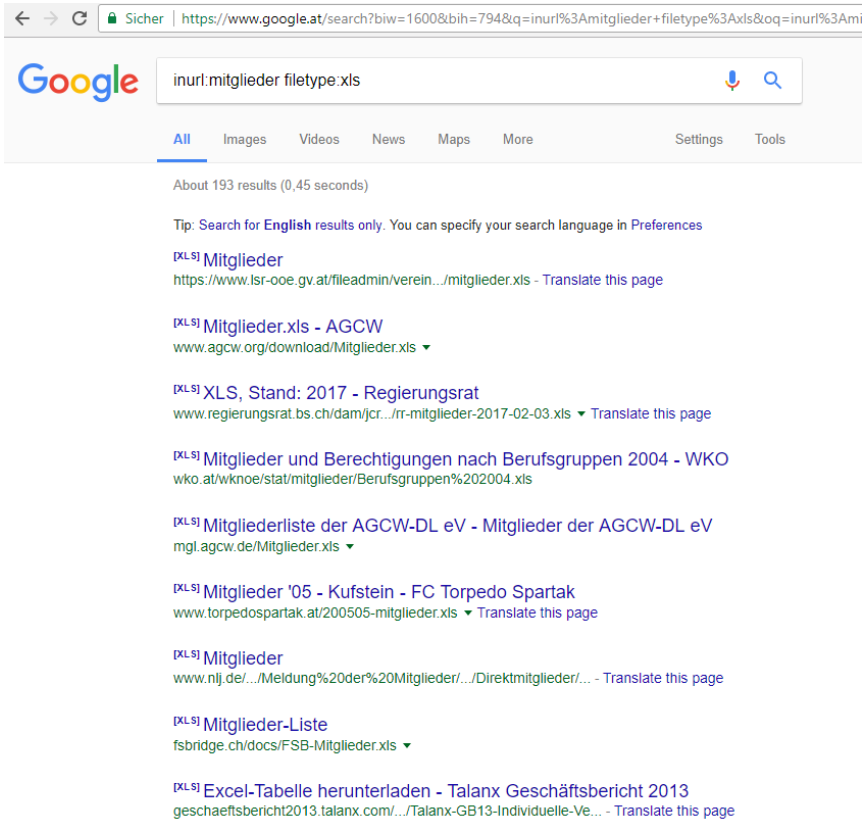
Was beide Parteien nicht wissen:

Eine unbefugte Person hört mit!

STEUERBERATER

Steuerberater beratet nach bestem Wissen und Gewissen.

Informationsgewinnung: Google-Hacking



Maßnahmen - Informationssicherheit

BEZEICHNUNG	ERKLÄRUNG
Hacking-Angriff simulieren	Laufende Sicherheitsüberprüfungen der IT-Infrastruktur ermöglichen das zeitnahe Erkennen und somit Beheben von Sicherheitslücken.
Bewusstseinsschaffung	Regelmäßiges Training und laufende Schulungen machen aus Ihren Mitarbeitern eine menschliche Firewall und diese werden Anweisungen via Telefon oder E-Mail kritischer hinterfragen.
Prüfung & Dokumentation	Regelmäßige Überprüfung der eigenen IT, Maßnahmen und Prozesse sowie die Dokumentation dieser ermöglicht die Verbesserung bestehender Maßnahmen.
Stand der Technik	Maßnahmen, Methoden und Lösungen nach dem Stand der Technik stellen einen Basisschutz für eine Vielzahl von Bedrohungsszenarien dar.
Kommunikationskultur	Häufig werden Sicherheitsvorfälle nicht erkannt, weil nicht über Verdachtsmomente gesprochen wird. Ermutigen Sie Ihre Mitarbeiter offen über Sicherheitsthemen zu sprechen.

Maßnahmen – EU-DSGVO

BEZEICHNUNG	ERKLÄRUNG
IST-Erhebung	Erheben Sie den IST-Stand in Ihrer Organisation und prüfen Sie den Handlungsbedarf, der sich aus der EU-DSGVO ergibt.
Maßnahmen	Definieren und planen Sie konkrete technische und organisatorische Maßnahmen sowie Arbeitspakete, die zur einer erfolgreichen Umsetzung der Anforderungen durchzuführen sind.
Verzeichnis der Verarbeitungstätigkeiten	Erstellen Sie die erste Version Ihres Verzeichnisses für Verarbeitungstätigkeiten auf Basis Ihrer Geschäftsprozesse.
Datenschutz-Folgeabschätzung	Prüfen Sie die Notwendigkeit zur Durchführung einer Datenschutzfolgeabschätzung für alle Ihre Verarbeitungsvorgänge. Planen und führen Sie diese ggf. durch.
Betroffenenrechte	Erstellen Sie einen Prozess, wie Sie Auskunftsrecht, Löschrecht und die anderen Betroffenenrechte umsetzen. Testen Sie die Umsetzung anhand eines Planspieles.
Datenschutzbeauftragter	Prüfen Sie die Notwendigkeit zur Benennung eines Datenschutzbeauftragen. Müssen oder wollen Sie einen internen oder externen benennen, stellen Sie dessen Qualifikation sicher und kommunizieren Sie die Kontaktdaten an die Behörde.

Wir freuen uns auf die Zusammenarbeit!

Das Angebot an Dienstleistern für Human Resources, Engineering, Training und Education, Netzwerk- und IT-Security ist groß,…

…aber wir vereinen all diese Kernkompetenzen zum einzigartigen Nutzen für Sie!