



Fachveranstaltung für Energie. Daten. Zukunft.

Agenda

Begrüssung und Einleitung

Martin Simioni CEO EKT-Gruppe

Cyberangriffe gegen die Schweiz:

Schutzmassnahmen des Bundes für kritische Infrastrukturen

Nathalie Grätzer Projektleiterin Nationale Cybersicherheitsstrategie NCS

Alarmstufe rot: Cyberangriff!

Erlebnisbericht einer realen Cyberattacke

Andreas Plüer Bereichsleiter Digital Services, EKT AG

Neues Datenschutzgesetz:

Was ändert sich und worauf sollte geachtet werden?

Dr. Nicolas Huber Leiter Compliance & Qualität, EKT AG

Zusammenfassung und Verabschiedung

Martin Simioni CEO EKT-Gruppe

Apéro riche

Begrüssung und Einleitung

Martin Simioni
CEO EKT-Gruppe

EKT EKT Dialog

Der Mantelerlass wurde verabschiedet.



SRF News Sport Meteo Kultur Dok Wissen

Parlament bereinigt Energie-Mantelerlass
Aus SRF 4 News aktuell vom 26.09.2023.
Bild: Keystone/Anthony Anex

News > Schweiz >

Sichere Stromversorgung Kompromiss beim Energie-Mantelerlass geglückt

Mit dem Ja zum Energie-Mantelerlass schiebt das Parlament jetzt die sichere Stromversorgung in der Energiewende an.

Dienstag, 26.09.2023, 14:04 Uhr

EKT EKT Dialog

Blick

DE | FR

Politik | Über das Stromversorgungsgesetz soll das Stimmvolk entscheiden

Referendum gegen Röstis Mantelerlass

«Die Natur wird der Energieproduktion geopfert»

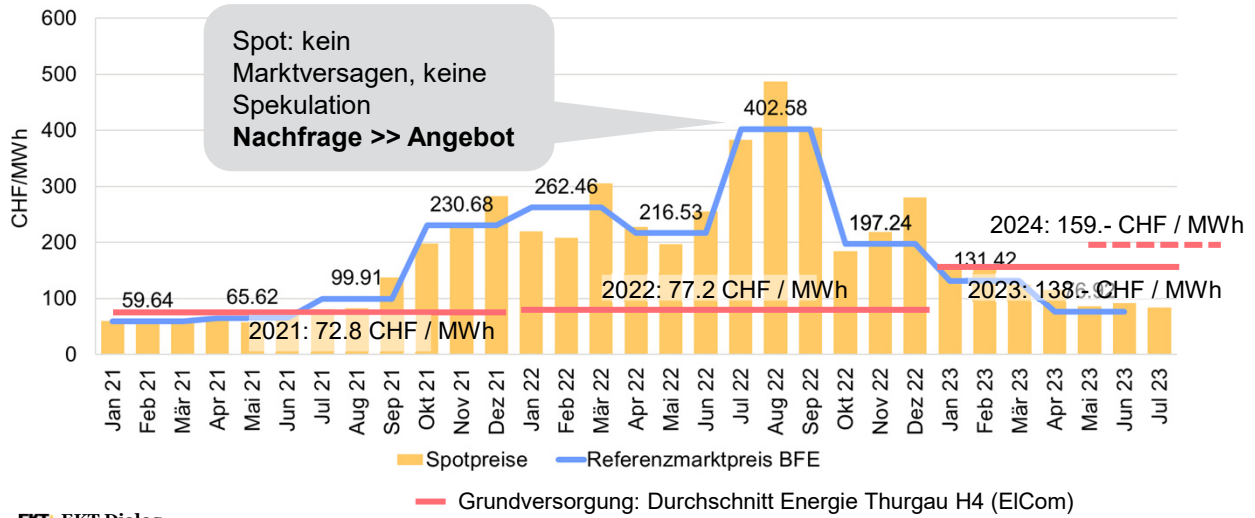
Das Volk soll entscheiden über das Gesetz über eine sichere Stromversorgung mit erneuerbaren Energien. Ein neu gegründetes Bündnis hat ein Referendum lanciert. Es moniert, dass mit diesem Mantelerlass der Schutz von Natur und Landschaft auf der Strecke bleibe.

Publiziert: 10.10.2023 um 12:10 Uhr



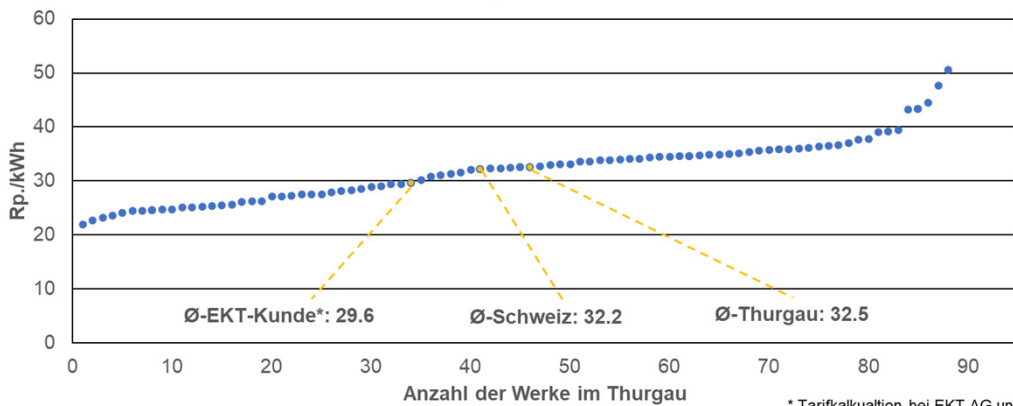
47

Starre Grundversorgungstarife setzen Fehlanreize, blockieren Informationsfluss



Ausblick Tarife 2024

Totaltarif 2024 EVU-Thurgau, Ø-EKT-Kunde* und Ø-Schweiz
EiCom-Verbrauchskategorie H4, Standardprodukt

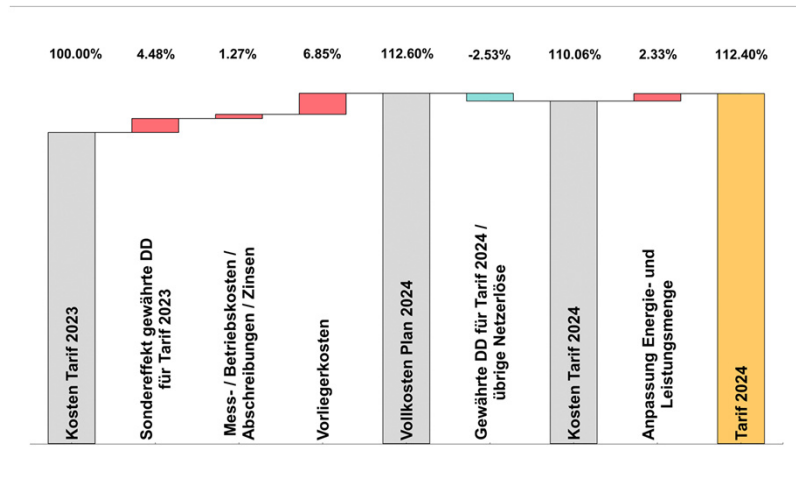


* Tarifkalkulation bei EKT AG und ELV 2024 bei EKT Energie AG
→ Marktanteil rund 24%

EKT: EKT Dialog

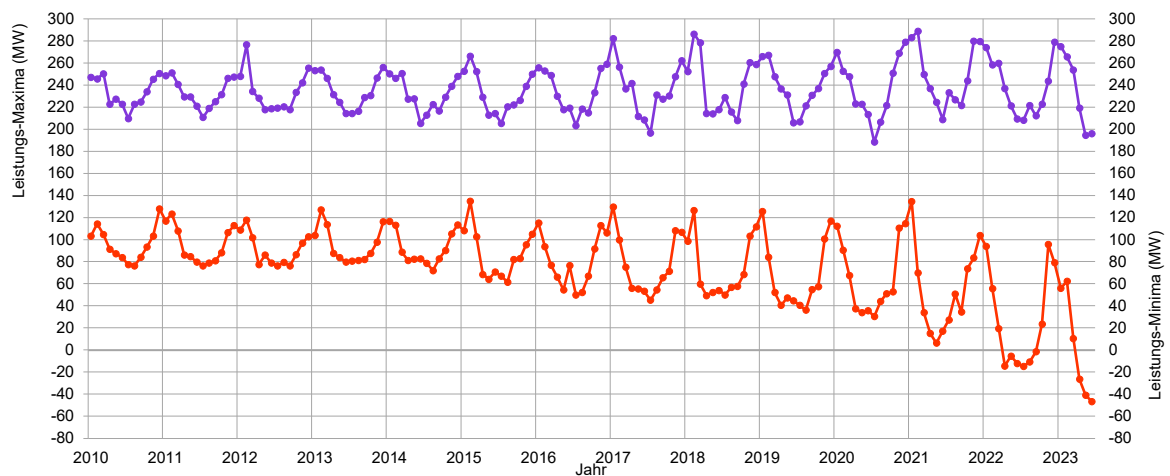
EKT-Netztarife 2024

Vorlieger als Kostentreiber



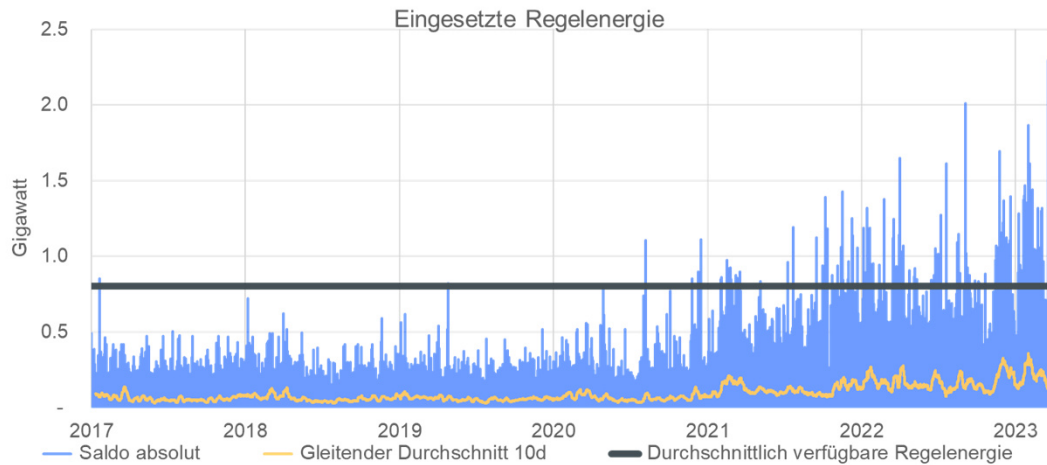
EKT EKT Dialog

Leistungsminima und -maxima (Nettobezug /-einspeisung NE 3)



EKT EKT Dialog

Regelenergieverbrauch und –kosten nehmen stark zu



EKT: EKT Dialog

EKT beteiligt sich mit 50% an Windprojekt auf dem Wellenberg in Thundorf



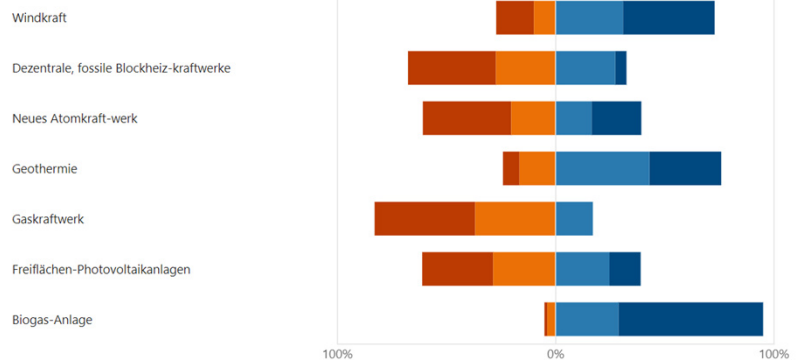
- Nur noch drei statt acht Windanlagen
- Einfluss auf Landschaft und Umwelt erheblich reduziert
- Mindestabstand 850 m gemäss Gemeindeversammlung vom 27.4.2023
- Wirtschaftlichkeit nur gegeben dank KEV-Zusage
- 2024 Gemeindeabstimmung
- Vorbehältlich Zustimmung Regierungsrat

EKT: EKT Dialog

Biogas, Geothermie und Windkraft bei Landwirten bevorzugt

«Wenn der Kanton Thurgau seine Winterstromproduktion ausbauen müsste: wie ist Ihre Position zur Realisierung der folgenden Anlagen in Ihrer Gemeinde?»

■ Deutliche Ablehnung ■ Ablehnung ■ Zustimmung ■ Deutliche Zustimmung



EKT EKT Dialog

Windkraft im Detail

«Befürworten Sie, dass die EKT in Ihrer Gemeinde Windkraft-anlagen baut und betreibt?»

■ Strikt dagegen ■ Dagegen ■ Neutral ■ Dafür ■ Sehr dafür



EKT EKT Dialog

Die Gesetze werden in Bern gemacht. Aber über unsere Energiezukunft entscheiden die Gemeinden und ihre Bürger.

EKT EKT Dialog

Cyberangriffe gegen die Schweiz: Schutzmassnahmen des Bundes für kritische Infrastrukturen

Nathalie Gratzer

Bundesamt für wirtschaftliche Landesversorgung BWL
Projektleiterin Nationale Cybersicherheitsstrategie NCS

EKT EKT Dialog

IKT Minimalstandard



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung EDB
Bundesamt für Wirtschaftliche Landesversorgung BWL
Fachwissen IKT

IKT-Minimalstandard - Assessment Tool

Version 1.11 April 2023 - Update NIST SP 800-53 Rev 5 - ISO 27001:2022

Aufbau und Einfeldung zum Rechenzentrum

Das Assessment-Tool besteht aus 6 Programmen (Erfassung, Assessment, Resultate und Reporting). Um das eigene Rechenzentrum einschätzen zu können, alle 50 Kriterien im Daten "Assessment" eingetragt. Checken Sie die Spalte D (Bewertung) für die entsprechende Daten- und Informationssystem-Bereich den entsprechenden Wert auszuwählen.



Die Definition der Werte (1 bis 5) kann dem Reiter "Bewertungen" entnommen werden. In der rechtsseitigen Spalte "Kommentare" begründen Sie das definierte Maturitätsniveau für alle 50 Kriterien.

Darstellung der Resultate

Nachdem alle 50 Kriterien bewertet wurden, werden die Resultate im Reiter "Resultate" dargestellt. Die Resultate im Reiter "Overall Cyber Security Maturity Rating" geben ein überblicks Resultat zu dem Cybersicherheits (Cyber-Security) Frameworks an. Das IKT-Minimalstandard ist dabei als Referenzwert dargestellt. Das "Overall Cyber Security Maturity Rating" den Maturitätsniveau (Maturitätsniveau) darstellt.



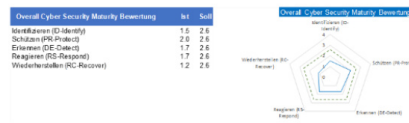
EKT EKT Dialog

Cyber Security Beratung EKT Digital Services IKT Minimalstandard

Quick-Win-Empfehlungen aus der Selbsteinschätzung

Empfehlung	Umfeld	ICM	IS	IS	IS	IS	IS
1. Identifizieren Sie die wichtigsten Assets und Daten...							
2. Implementieren Sie eine Multi-Faktor-Authentifizierung...							
3. Erstellen Sie ein Notfallwiederherstellungsplan...							
4. Implementieren Sie eine Patch-Management-Prozess...							
5. Implementieren Sie eine Sicherheitsbewertung...							
6. Implementieren Sie eine Sicherheitsbewertung...							
7. Implementieren Sie eine Sicherheitsbewertung...							
8. Implementieren Sie eine Sicherheitsbewertung...							
9. Implementieren Sie eine Sicherheitsbewertung...							
10. Implementieren Sie eine Sicherheitsbewertung...							

Cyber Security Resilienz aus IKT Minimalstandard

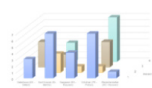


Ausführlicher Beratungsbericht

6. Empfehlungen

Die Empfehlungen sind hier in verschiedene Abschnitte geordnet. Im ersten Kapitel wird eine dringende Empfehlung für eine unverzügliche Einführung von Multi-Faktor-Authentifizierung ausgesprochen, gefolgt von den nach Prioritäten geordneten, weiteren Massnahmen zur Erhöhung der Resilienz gegen Cyberangriffe. Mit 27 empfohlenen Massnahmen sind über die Hälfte als Priorität 1 oder 2 einzustufen, d.h. hier ist das Verhältnis zwischen Aufwand und erwarteter Erhöhung der Cyberresilienz unserer Meinung nach positiv.

Empfehlung	Priorität
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1
17	1
18	1
19	1
20	1
21	1
22	1
23	1
24	1
25	1
26	1
27	1



EKT EKT Dialog

Alarmstufe rot: Cyberangriff! Erlebnisbericht einer realen Cyberattacke.

Andreas Plüer

Bereichsleiter Digital Services, EKT AG

EKT EKT Dialog

Alarmstufe rot: Cyberangriff!

- Was ist bei der Cyberattacke passiert?
- Weshalb war der Cyberangriff erfolgreich?
- Welche Vorkehrungen erschweren Cyberangriffe?

EKT EKT Dialog

Ruhe vor dem Sturm



Quelle: shanemyersphoto



Quelle: LAAX / Danuser

EKT EKT Dialog

Die SMS, mit der mein Alptraum begann...










EKT EKT Dialog

Ein Cyberangriff!



EKT: EKT Dialog

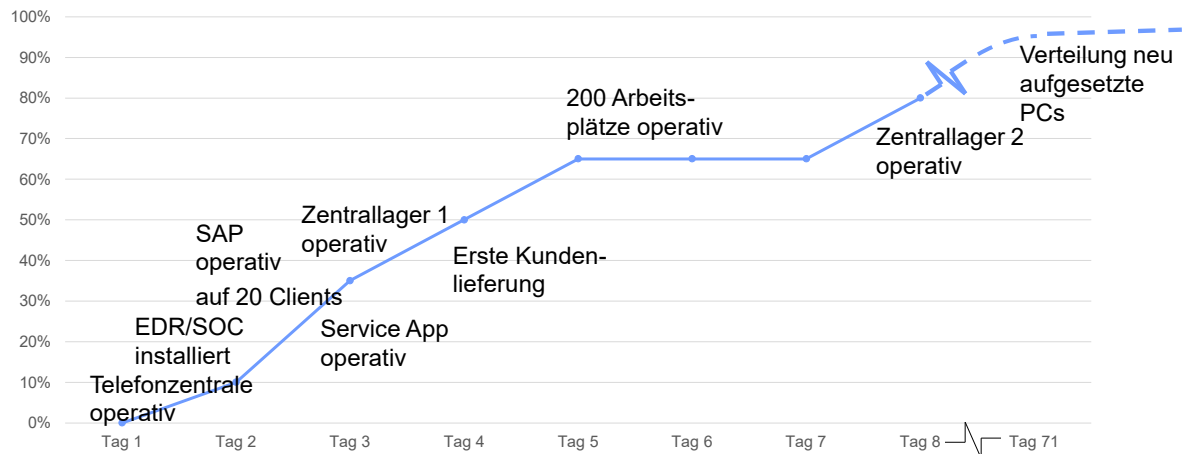
Zeitlicher Ablauf Cyberangriff 23./24.07.19

- 
Ungewöhnliches Verhalten IT-Überwachungssysteme festgestellt, unübersichtliche Gesamtlage für IT-Dienstleister, Eskalation innerhalb Pikettorganisation
- 
Befund: Malware-Attacke! Sofortiges Herunterfahren aller Systeme. Alarmierung Kunde (CIO-Stv. , CFO)
- 
Geschäftsleitung durch CFO informiert
- 
Krisenstab einberufen, Information der Führungskräfte, Bezug «War Room»
- 
CIO eingetroffen, erste Krisenstabsitzung zur Lagebeurteilung, Beschluss von Sofortmassnahmen
- 
Schadensbild ermittelt, externe Cyber Security Spezialisten aufgeboden
- 
Priorisierung erstellt, Wiederherstellungsarbeiten gestartet

EKT: EKT Dialog

Krisenbewältigung – auf der Zeitachse

Liefer- und Servicebereitschaft in %

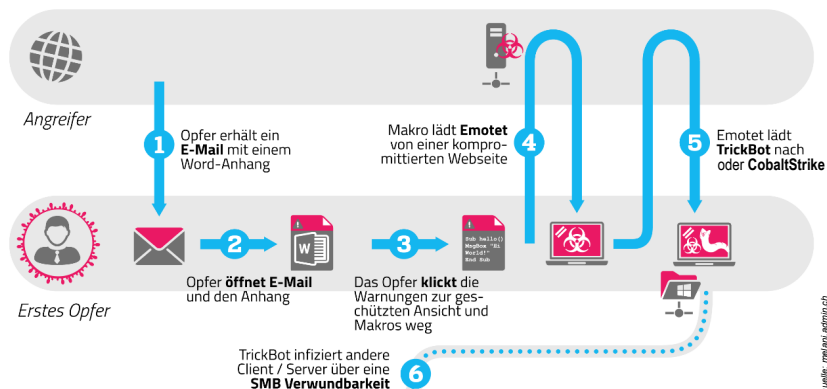


EKT: EKT Dialog

Das Vorgehen der Angreifer

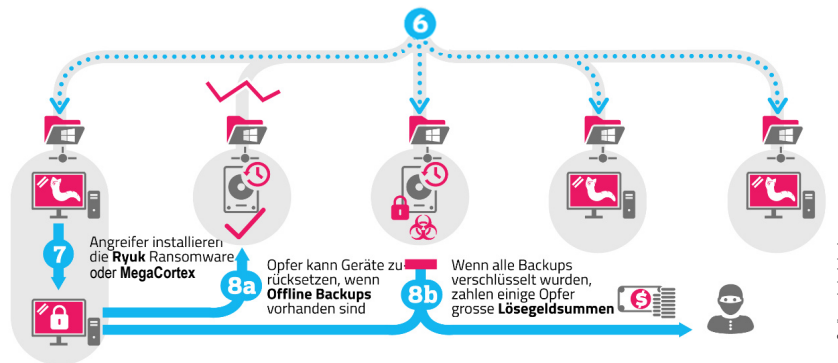
Emotet Infektionsablauf

Attribution
CC BY @CERT.ch



EKT: EKT Dialog

Das Vorgehen der Angreifer



EKT EKT Dialog

Alarmstufe rot: Cyberangriff!

- Was ist bei der Cyberattacke passiert?
- **Weshalb war der Cyberangriff erfolgreich?**
- Welche Vorkehrungen erschweren Cyberangriffe?

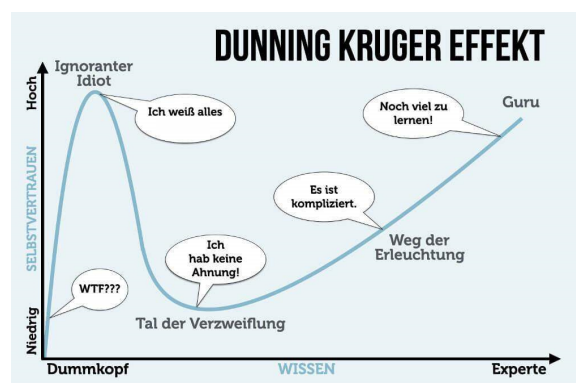
EKT EKT Dialog

Publikumsumfrage

Glauben sie, dass sie zu den schlechteren 50 Prozent der Autofahrenden in diesem Raum gehören?

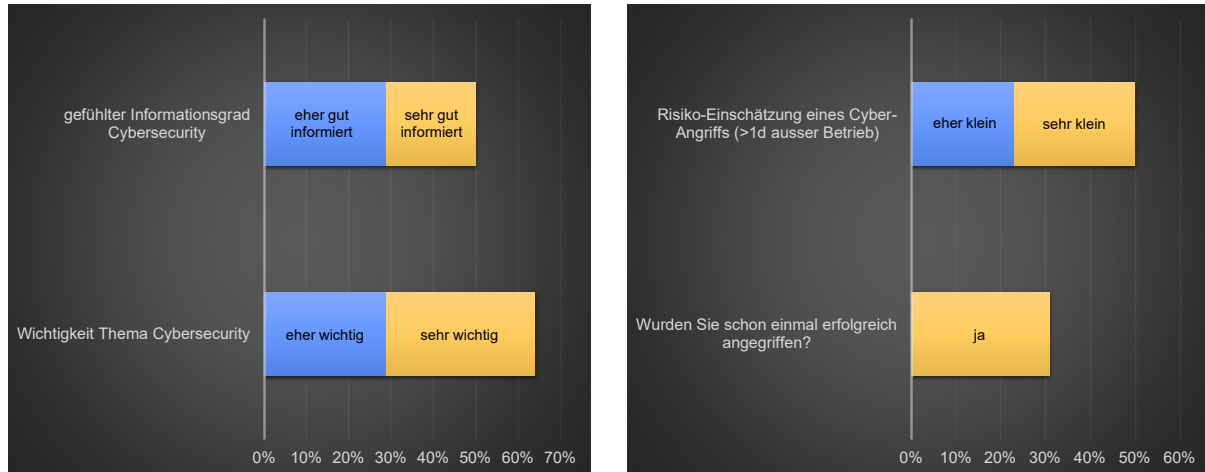
EKT: EKT Dialog

Exkurs zum Thema «Selbstüberschätzung»



EKT: EKT Dialog

Exkurs zum Thema «Selbstüberschätzung» Studie GFS Zürich (2022, n=504 KMU)



EKT: EKT Dialog

Fehleinschätzungen im Vorfeld – Klartext

Unsere Unternehmung ist in einer traditionellen Branche in der Schweiz tätig. Wir sind keine Bank und stehen nicht im Fokus von Cyberangriffen. Weshalb sollen wir auch ein lukratives Ziel für Hacker sein?



EKT: EKT Dialog

Fehleinschätzungen im Vorfeld – Klartext

Unsere Perimetersicherheit mit Firewalls, Virens Scanner, Anti-Spam-Lösungen etc. ist auf einem top Stand. Server und Clients auf neuestem Betriebssystem und regelmässig gepatched, alles über dem Branchendurchschnitt. Bisher wurde noch jeder Angriff erfolgreich abgewehrt!

EKT: EKT Dialog

Fehleinschätzungen im Vorfeld – Klartext

Wir führten eine 2-monatige Cybercrime Awareness-Kampagne mit allen 1'200 Mitarbeitenden mit simulierten Phishing-Mails durch. Bei uns fällt doch niemand mehr auf Phishing rein!

EKT: EKT Dialog

Fehleinschätzungen im Vorfeld – Klartext

Unsere IT wird im Outsourcing durch absolute Profis betrieben. Alles sicher, die machen nichts anderes, den ganzen Tag!



EKT: EKT Dialog

Fehleinschätzungen im Vorfeld – Klartext

Ich lese ja regelmässig über diese Cyberangriffe und muss meine Geschäftsleitung immer wieder über meine Lageeinschätzung informieren. Ich kenne mich in diesem Thema Cyberkriminalität doch aus!



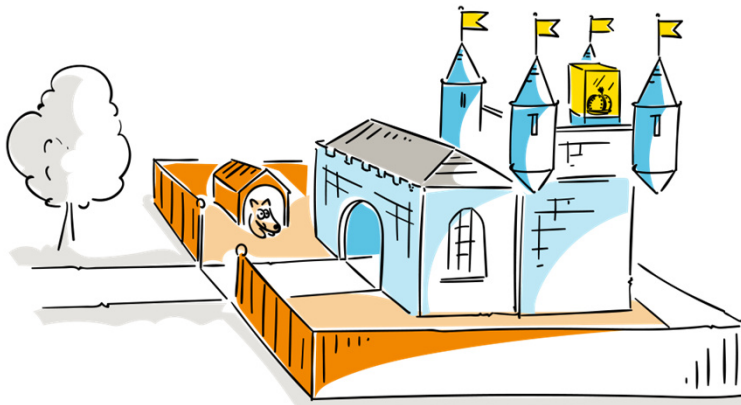
EKT: EKT Dialog

Alarmstufe rot: Cyberangriff!

- Was ist bei der Cyberattacke passiert?
- Weshalb war der Cyberangriff erfolgreich?
- Welche Vorkehrungen erschweren Cyberangriffe?

EKT: EKT Dialog

Welche Vorkehrungen erschweren Cyberangriffe? Klartext!



EKT: EKT Dialog

EKT:

Energie.
Daten.
Zukunft.

EKT AG
Bahnhofstrasse 37
9320 Arbon
T 071 440 61 11
info@ekt.ch
www.ekt.ch

Andreas Plüer
Bereichsleiter Digital Services
D 071 440 63 33
andreas.plueer@ekt.ch

EKT EKT Dialog

Neues Datenschutzgesetz: Was ändert sich und worauf sollte geachtet werden?

Dr. Nicolas Huber
Leiter Compliance & Qualität, EKT AG

EKT EKT Dialog

Relevante Neuerungen

EKT EKT Dialog

Grundlegende Bestrebungen

- **Gesamthaft: Selbstregulierung, risikobasierter Ansatz**
- Verbesserung der Transparenz
- Stärkung des Eidgenössischen Datenschutzbeauftragten (EDÖB)
- Verschärfung der Strafbestimmungen
- «Privacy by Design» und «Privacy by Default»
- Datenschutz-Folgenabschätzung
- Datenherausgabe und -übertragung
- Förderung der Datensicherheit

Die nachfolgenden Auszüge aus dem Bundesgesetz über den Datenschutz, SR. 235.1 (Datenschutzgesetz, DSG) dienen der Illustration und bilden die einzelnen Artikel nicht vollständig ab.

EKT EKT Dialog

Verbesserung der Transparenz

- **Ausgeweitete aktive Informationspflicht**
 - Neu grundsätzlich bei jeder Beschaffung von Personendaten
 - Mindestangaben
 - Identität und Kontakt
 - Zweck
 - Allfällige Empfänger
 - Ausnahmen
 - Betroffene verfügen bereits über Information
 - Bearbeitung gesetzlich vorgesehen
 - Gesetzliche Geheimhaltungspflicht
 - Bei indirekter Beschaffung
 - Information ist unmöglich/unverhältnismässig
 - Einschränkung/Aufschub/Verzicht bei überwiegenden Interessen

EKT EKT Dialog

Art. 19 Informationspflicht bei der Beschaffung von Personendaten

¹ Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

² Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

³ Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr zudem die Kategorien der bearbeiteten Personendaten mit.

⁴ Werden die Personendaten ins Ausland bekanntgegeben, so teilt er der betroffenen Person auch den Staat oder das internationale Organ und gegebenenfalls die Garantien nach Artikel 16 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 17 mit.

⁵ Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr die Informationen nach den Absätzen 2–4 spätestens einen Monat, nachdem er die Daten erhalten hat, mit. Gibt der Verantwortliche die Personendaten vor Ablauf dieser Frist bekannt, so informiert er die betroffene Person spätestens im Zeitpunkt der Bekanntgabe.

Verbesserung der Transparenz

- **Automatisierte Einzelentscheidung**
 - Entscheidung ausschliesslich automatisiert
 - Folge für Betroffene
 - Gewisse Komplexität, Bewertung, Interpretation
 - Information über Logik hinter der Entscheidung
 - Entscheidungsfreiheit für Verantwortlichen bleibt bestehen

EKT EKT Dialog

Art. 21 Informationspflicht bei einer automatisierten Einzelentscheidung

¹ Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (automatisierte Einzelentscheidung).

² Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.

³ Die Absätze 1 und 2 gelten nicht, wenn:

- a. die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder
- b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

Verbesserung der Transparenz

- **Ausgeweitetes Auskunftsrecht**
 - Ergänzung zur Informationspflicht
 - Leicht erweiterter Katalog
 - Weitergehende Informationen über Generalklausel «diejenigen Informationen, die erforderlich sind»
 - Nicht ganze Dokumente, nur Personendaten «als solche»
 - Keine «Beweisbeschaffung»
 - Einschränkung
 - Gesetzlich, bspw. Berufsgeheimnis
 - Überwiegende Interessen
 - Querulatorisch

Art. 25 Auskunftsrecht

¹ Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

² Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
- b. die bearbeiteten Personendaten als solche;
- c. der Bearbeitungszweck;
- d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer;
- e. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;
- f. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;
- g. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Artikel 19 Absatz 4.

EKT EKT Dialog

Verbesserung der Transparenz

- **Bearbeitungsverzeichnis**
 - Ausnahme
 - Weniger als 250 Mitarbeitende
 - Keine besonders schützenswerten Personendaten in grossem Umfang
 - Kein Profiling mit hohem Risiko
 - Lohnt sich auch ohne gesetzliche Pflicht
- **Zusammenfassung sachlich zusammenhängender Bearbeitungen zulässig**
- **Sicherstellung der Datenschutz-Compliance**
- **Enthält selbst keine Personendaten**

Art. 12 Verzeichnis der Bearbeitungstätigkeiten

¹ Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.

² Das Verzeichnis des Verantwortlichen enthält mindestens:

- a. die Identität des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
- d. die Kategorien der Empfängerinnen und Empfänger;
- e. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
- f. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8;
- g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

EKT EKT Dialog

Stärkung des EDÖB

- Untersuchung von Amtes wegen oder auf Anzeige
 - Mitwirkungspflichten
 - Zwangsmassnahmen
- Verfügungen anstatt Empfehlungen
 - Anpassungen
 - Unterbruch
 - Abbruch
 - Löschung

Art. 49 Untersuchung

¹ Der EDÖB eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.

² Er kann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist.

Art. 50 Befugnisse

¹ Kommt das Bundesorgan oder die private Person den Mitwirkungspflichten nicht nach, so kann der EDÖB im Rahmen der Untersuchung insbesondere Folgendes anordnen:

- a. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die für die Untersuchung erforderlich sind;
- b. Zugang zu Räumlichkeiten und Anlagen;
- c. Zeugeneinvernahmen;
- d. Begutachtungen durch Sachverständige.

² Das Berufsgeheimnis bleibt vorbehalten.

³ Zum Vollzug der Massnahmen nach Absatz 1 kann der EDÖB andere Bundesbehörden sowie die kantonalen oder kommunalen Polizeiorgane beiziehen.

EKT EKT Dialog

Verschärfung der Strafbestimmungen

- Erhöhung Bussenobergrenze von CHF 10'000.- auf CHF 250'000.-
- Verfolgung bei den Kantonen
 - EDÖB kann Anzeige erstatten
- Primärer Adressat sind Menschen und nicht Unternehmen
 - Organe, Gesellschafter, leitende Angestellte

Art. 60 Verletzung von Informations-, Auskunft- und Mitwirkungspflichten

¹ Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

- a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;
- b. die es vorsätzlich unterlassen:
 1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder
 2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

² Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoß gegen Artikel 49 Absatz 3 dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

EKT EKT Dialog

«Privacy by Design» und «Privacy by Default»

- Implementierung des Datenschutzes bereits zu Beginn einer Datenbearbeitung
- Bei Wahlmöglichkeiten für Betroffene, datenschutzfreundlichste als Grundeinstellung

Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

¹ Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

² Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

³ Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

EKT EKT Dialog

Datenschutz-Folgenabschätzung

- Instrument zur Selbstkontrolle
- Datenbearbeitung die ein hohes Risiko für die Persönlichkeit der Betroffenen mit sich bringen
- Beschreibung der Risiken
- Bewertung der Risiken
 - Risikomatrix (Schwere * Eintretenswahrscheinlichkeit)
- Massnahmen zur Senkung der Risiken
- Bei hohem Nettorisiko nach Massnahmen Stellungnahme EDÖB einholen
- Ausnahme gesetzliche Verpflichtung
 - Z.B. Daten aus Smart Metering gemäss StromVV

Art. 22 Datenschutz-Folgenabschätzung

¹ Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

² Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

- a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
- b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

³ Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

⁴ Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind.

⁵ Der private Verantwortliche kann von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 zertifiziert ist, oder wenn er einen Verhaltenskodex nach Artikel 11 einhält, der die folgenden Voraussetzungen erfüllt:

EKT EKT Dialog

Datenherausgabe und -übertragung

- Bekannt oder zugänglich gemachte Daten der Betroffenen
 - Automatisierte Bearbeitung
 - Einwilligung oder Zusammenhang mit Vertrag
- Herausgabe von Daten, welche eine Person betreffen
- Übertrag von Daten, welche eine Person betreffen an einen anderen Datenbearbeiter
- Stärkung des Wettbewerbs als Ziel
 - Konsumentenschutz
- Pflicht für Verteilnetzbetreiber zum Datenexport nach StromVV

Art. 28 Recht auf Datenherausgabe oder -übertragung

¹ Jede Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen, wenn:

- a. der Verantwortliche die Daten automatisiert bearbeitet; und
- b. die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.

² Die betroffene Person kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen überträgt, wenn die Voraussetzungen nach Absatz 1 erfüllt sind und dies keinen unverhältnismässigen Aufwand erfordert.

³ Der Verantwortliche muss die Personendaten kostenlos herausgeben oder übertragen. Der Bundesrat kann Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.

EKT EKT Dialog

Förderung der Datensicherheit

- Ausführliche Bestimmungen zur Sicherstellung einer angemessenen Datensicherheit in der neuen Datenschutzverordnung (DSV)
 - Technische und organisatorische Massnahmen («TOMs»)
 - Protokollierung
 - Bearbeitungsreglement
 - Bekanntgabe ins Ausland

Art. 1 Grundsätze

¹ Zur Gewährleistung einer angemessenen Datensicherheit müssen der Verantwortliche und der Auftragsbearbeiter den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen.

² Der Schutzbedarf der Personendaten wird nach den folgenden Kriterien beurteilt:

- a. Art der bearbeiteten Daten;
- b. Zweck, Art, Umfang und Umstände der Bearbeitung.

³ Das Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person wird nach den folgenden Kriterien beurteilt:

- a. Ursachen des Risikos;
- b. hauptsächliche Gefahren;
- c. ergriffene oder vorgesehene Massnahmen, um das Risiko zu verringern;
- d. Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen.

EKT EKT Dialog

Förderung der Datensicherheit

- Meldung von Verletzung der Datensicherheit
 - Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit
 - Bspw. Entwendung oder Löschung von Daten
 - Nur bei hohem Risiko für Betroffene
 - Information Betroffene, wenn zum Schutz erforderlich
 - Parallel Meldung an NCSC bei Cyberangriff

Art. 24 Meldung von Verletzungen der Datensicherheit

¹ Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

² In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

³ Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

⁴ Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

⁵ Er kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn:

- a. ein Grund nach Artikel 26 Absatz 1 Buchstabe b oder Absatz 2 Buchstabe b vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet;
- b. die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert; oder
- c. die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.

Spezifische Themen EVU

Hoheitliche Tätigkeit

- DSG gilt für Bearbeitung von Personendaten durch private Personen und Bundesorgane
- Kantonale Organe unterstehen den kantonalen Datenschutzgesetzen
- Wahrnehmung öffentlicher Aufgaben kann zur Qualifikation als Bundesorgan oder kantonales Organ führen
- Verschiedene Datenschutzgesetze für verschiedene Tätigkeiten
- Jemand ist kein Organ, sondern handelt als Organ
 - «*Bundesorgan*: Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist» (Art. 5 lit. i DSG)

EKT EKT Dialog

Smart Metering

- Regelung im StromVG (Art. 17a ff.) und StromVV (Art. 8a ff.)
- Personendaten dürfen für definierte Zwecke bearbeitet werden
- Personendaten dürfen an definierte Empfänger weitergegeben werden
- Weitergehende Bearbeitung
 - DSFA
 - Profiling
- Anwendbares Recht: DSG (Art. 17c StromVG)
 - Aufsichtsbehörde: kantonal

Art. 8d⁵⁹ Umgang mit Daten aus intelligenten Mess-, Steuer- und Regelsystemen

¹ Netzbetreiber dürfen die Daten aus dem Einsatz von Mess-, Steuer- und Regelsystemen ohne Einwilligung der betroffenen Person zu folgenden Zwecken bearbeiten:

- a. Personendaten sowie Daten juristischer Personen in pseudonymisierter Form, einschliesslich Lastgangwerten von fünfzehn Minuten und mehr: für die Messung, Steuerung und Regelung, für den Einsatz von Tarifsystemen sowie für den sicheren, leistungsfähigen und effizienten Netzbetrieb, die Netzbilanzierung und die Netzplanung;
- b. Personendaten sowie Daten juristischer Personen in nicht pseudonymisierter Form, einschliesslich Lastgangwerten von fünfzehn Minuten und mehr: für die Abrechnung der Energielieferung, des Netznutzungsentgelts und der Vergütung für den Einsatz von Steuer- und Regelsystemen.⁶⁰

² Sie dürfen die Daten aus dem Einsatz von Messsystemen ohne Einwilligung der betroffenen Person folgenden Personen weitergeben:

- a.⁶¹ Personendaten sowie Daten juristischer Personen in pseudonymisierter oder geeignet aggregierter Form: den Beteiligten nach Artikel 8 Absatz 3;
- b. die Informationen zur Entschlüsselung der Pseudonyme: den Energielieferanten des betreffenden Endverbrauchers.

EKT EKT Dialog

EKT:

Energie.
Daten.
Zukunft.

EKT AG
Bahnhofstrasse 37
9320 Arbon
T 071 440 61 11
info@ekt.ch
www.ekt.ch

Dr. iur. Nicolas Huber
Leiter Compliance & Qualität
EKT-Gruppe
D 071 440 62 03
nicolas.huber@ekt.ch

EKT EKT Dialog

Fragen und Antworten



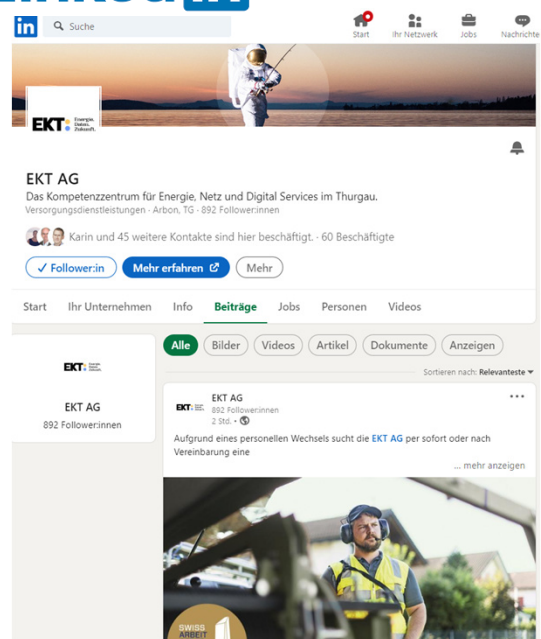
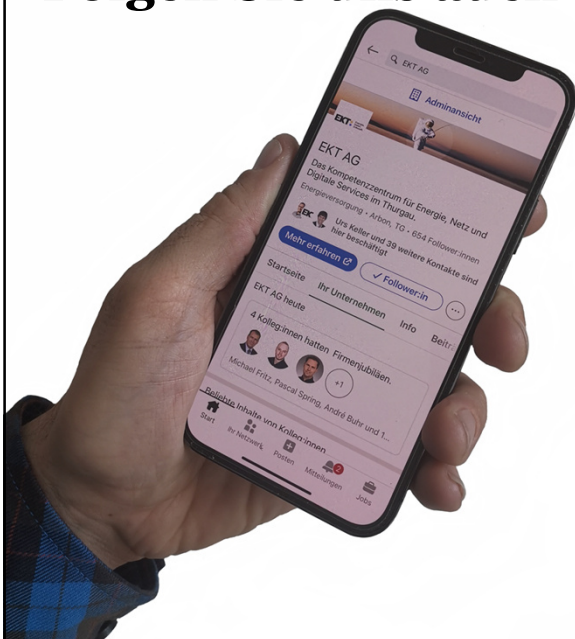
EKT EKT Dialog

Zusammenfassung und Verabschiedung

Martin Simioni
CEO EKT-Gruppe

EKT EKT Dialog

Folgen Sie uns auch auf **LinkedIn**



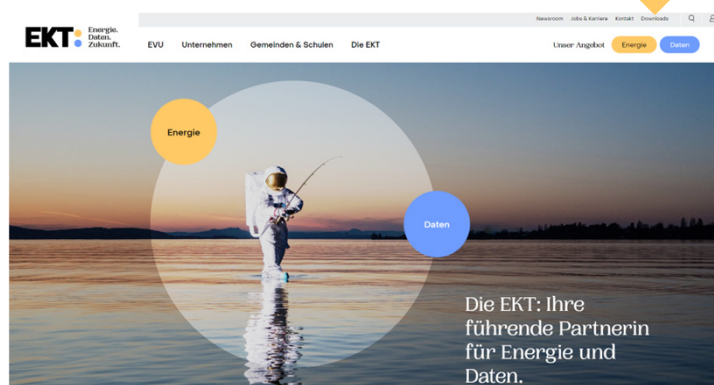
Umfrage zur Optimierung des EKT Dialog



EKT EKT Dialog

Präsentation zum Herunterladen

Auf www.ekt.ch finden Sie ab dem kommenden Montag die Präsentation dieses EKT Dialog als pdf-Datei zum Download.



EKT EKT Dialog

EKT:

Energie.
Daten.
Zukunft.

Herzlichen Dank für Ihre Aufmerksamkeit.

EKT AG
Bahnhofstrasse 37
9320 Arbon
T 071 440 61 11
info@ekt.ch
www.ekt.ch

EKT EKT Dialog

EKT:

Energie.
Daten.
Zukunft.

EKT Dialog



Fachveranstaltung für Energie. Daten. Zukunft.