EKT

Energie.
Daten.
Zukunft.

EKT: Gipfel – Digital Services

Agenda

- Rückblick
- Referat «Die Cyberpolizei der KAPO TG»
- Referat «KMU-taugliche Cybersecurity – aus Sicht der EKT»
- Zusammenfassung und Ausblick nächster Anlass
- Verabschiedung und Ausklang beim Frühstück

EKT: Gipfel
Rückblick 1. Gipfel 14.09.2022

EKT: Gipfel
Greifen Sie zu beim Frühstücksbuffet

- Während der Referate dürfen Sie ungezwungen essen, trinken und nachfassen
- Frisch zubereiteter Kaffee kann beim Personal bestellt werden
- Auch nach dem Abschluss des offiziellen Teils bleibt das Frühstücksbuffet für Sie weiter offen
- Für Fragen stehen wir gerne zur Verfügung

EKT: Gipfel
Überleitung zu den Referaten

Quelle: Adobe Stock #350976450

Referat «Die Cyberpolizei der KAPO TG»

Referat «KMU-taugliche Cybersecurity – aus Sicht der EKT»

- Andreas Plüer, Bereichsleiter Digital Services EKT AG

Agenda

- Cybersecurity aus Sicht der EKT
  - als Betreiberin Kritischer Infrastrukturen
  - als KMU
- Lösungsangebote von EKT Digital Services unter dem Namen «Protektor Services»

Ausgangslage: Schutzniveau Cybersecurity Kritische Infrastrukturen

Startseite | Wirtschaft | Umfrage zu Cyber-Sicherheit - Schweizer Stromversorger sind ungen

Umfrage zu Cyber-Sicherheit

Schweizer Stromversorger sind ungenügend gegen Hacker geschützt

Besonders schlecht sind die Firmen im Erkennen von Angriffen sowie bei der Reaktion darauf. Die europäische Konkurrenz schneidet bei der Cyber-Sicherheit besser ab.

Publiziert: 02.07.2021, 09:46

Neue Smart-Meter-Stromzähler in einem Mehrfamilienhaus. (Archivbild)
Foto: Gaetan Bally (Keystone)

Schweizer Stromversorger sind gemäss einer neuen Umfrage des Bundes nur ungenügend gegen Attacken aus dem

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Digital Innovation Office

Bericht vom 28 Juni 2021

Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung

Schliesslich ergibt sich im Bereich der IT-Sicherheit das folgende Bild über alle 124 Umfrageteilnehmer entlang der fünf IKT Minimalstandard Funktionen:

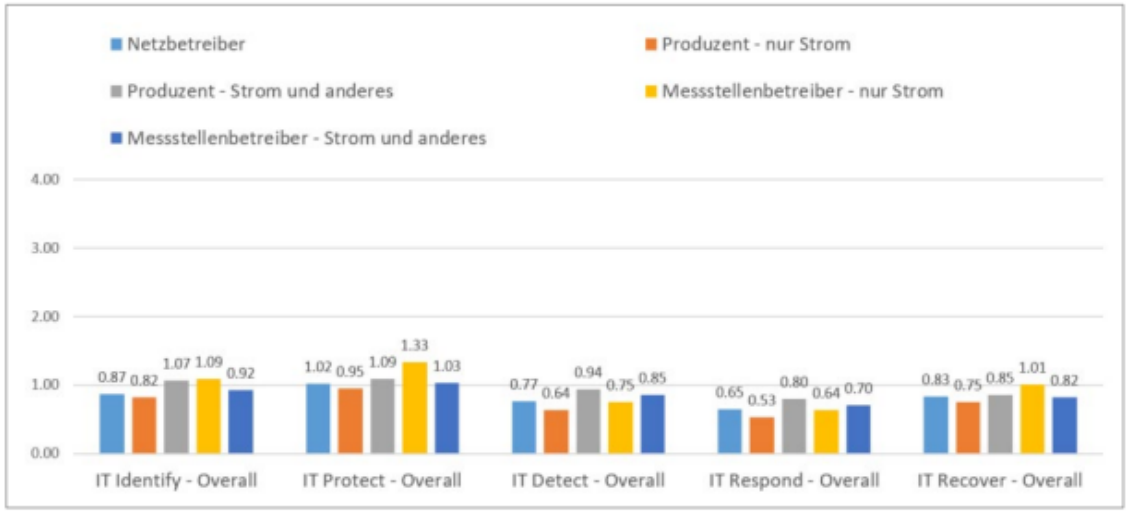
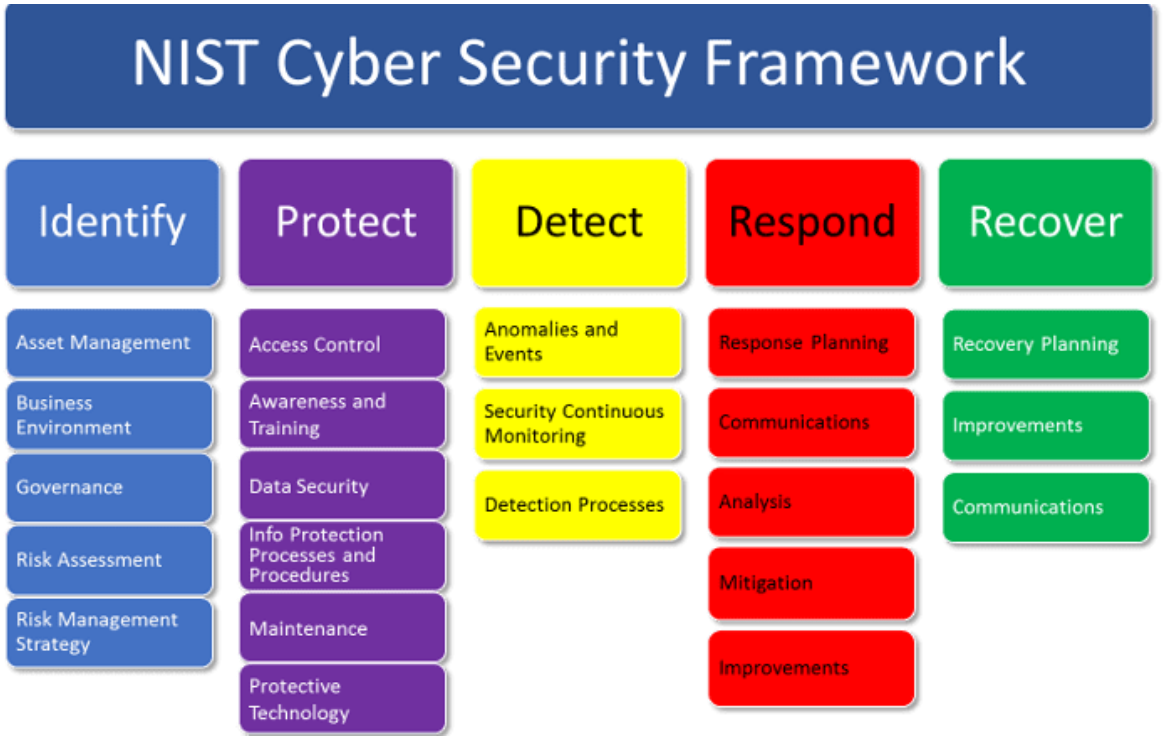


Abbildung 9: Maturität IT-Sicherheit

Der generelle Stand der Maturität ist sehr niedrig. Kaum eine Cyber-Fähigkeit erreicht einen Wert über der Maturitätsstufe 1, welche als rudimentäre Basisstufe gilt. Die Cyber-Risiken, werden so gemäss Auslegung, oftmals nur ad-hoc oder reaktiv verwaltet. Auch scheinen Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit des Öfteren als nicht formalisiert. Es ist davon auszugehen, dass aufgrund der fehlenden Prozessen keine abschliessende Sicht über die Sicherheitsrisiken innerhalb der IT-Landschaft gegeben ist.

Quelle: Bundesamt für Energie

NIST Cyber Security Framework
National Institute of Standards and Technology

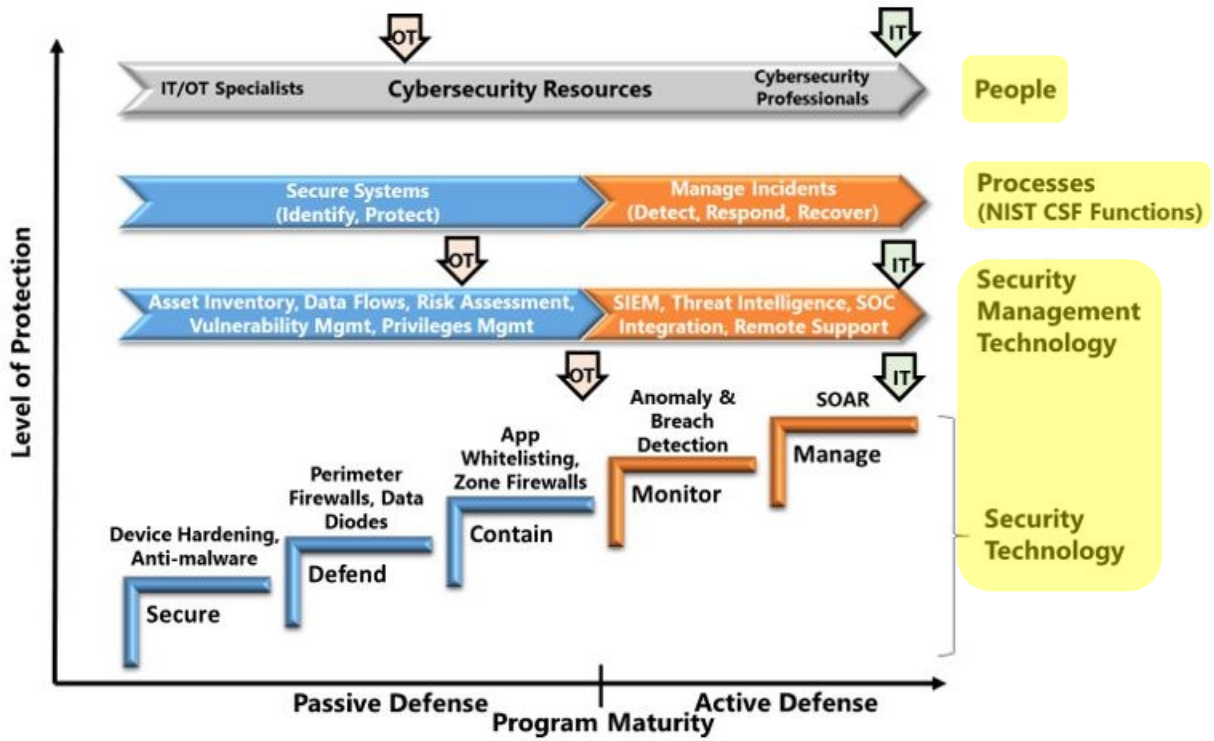


Quelle: https://www.darkreading.com/physical-security/a-guide-to-the-nist-cybersecurity-framework

Cybersecurity-Fähigkeiten:

- Identifizieren
- Schützen
- Erkennen
- Reagieren
- Wiederherstellen

Cybersecurity aus dem Blick der EKT als Betreiberin Kritischer Infrastrukturen



Quelle: https://www.arcweb.com/industry-best-practices/enabling-safe-secure-industrial-operations

ARC Cybersecurity Model Shows Current State of Industrial Cybersecurity Programs

Menschen

- Information Security Team (IST) mit Chief Information Security Officer (CISO) in der Organisation etabliert
- Trennung der operativen und strategischen Verantwortung für Informationssicherheit
- Regelmässige Awareness-Massnahmen

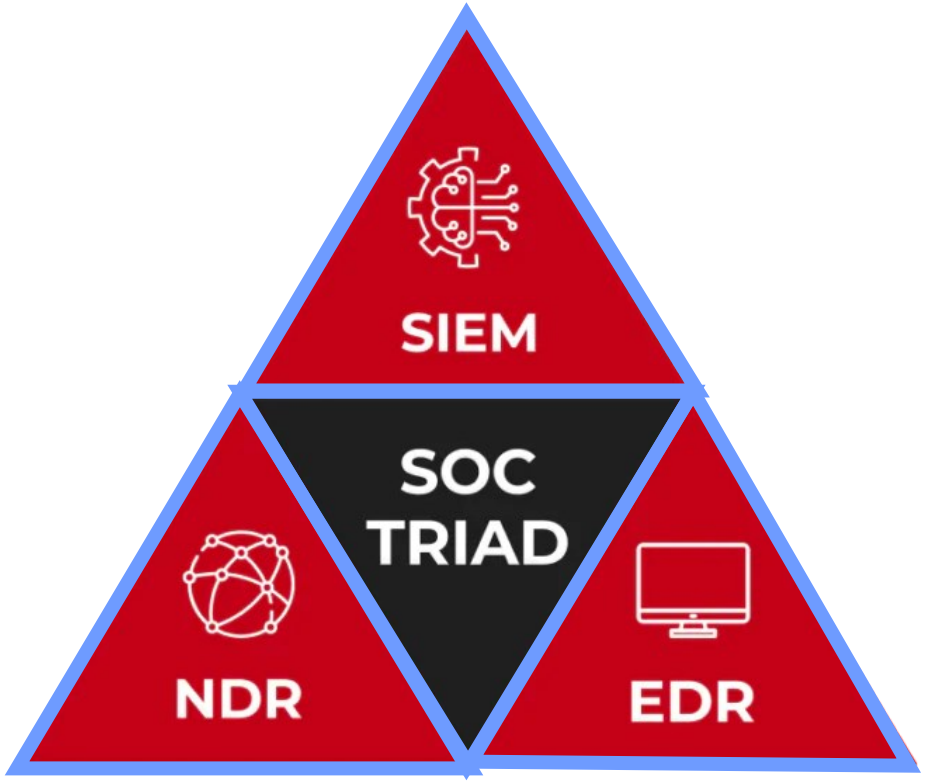
Prozesse

- Managementsystem für die Informationssicherheit (ISMS) auf Basis ISO 27001
- Security Operations Center-Prozesse (Detect, Respond, Recover) 7 x 24h durch externe Spezialisten

Technologien

- Firewalls, redundant und zu allen Zonenübergängen
- EDR (Endpoint Detection and Response)
- NDR (Network Detection and Response)
- SIEM (Security Information and Event Mgmt.)
- Zscaler, «VPN always on», gehärtete Endgeräte
- Netzwerkzonierung

Drei Eckpfeiler der SOC-Sichtbarkeitstriade: EDR+NDR+SIEM



Quelle: https://wizardcyber.com/what-is-the-soc-visibility-triad/

Security Operations Center

- Eine Zentrale, in der ein Informationssicherheits-Team Cybersicherheits-Ereignisse überwacht, erkennt, analysiert und behebt, in der Regel 365 Tage im Jahr rund um die Uhr.

Endpoint Detection and Response

- Systeme, die verdächtige Aktivitäten und ihre Ursachen auf einem Endgerät erkennen

Network Detection and Response

- Systeme, die den Netzwerkverkehr kontinuierlich überwachen und analysieren, um verdächtigen Datenverkehr zu erkennen

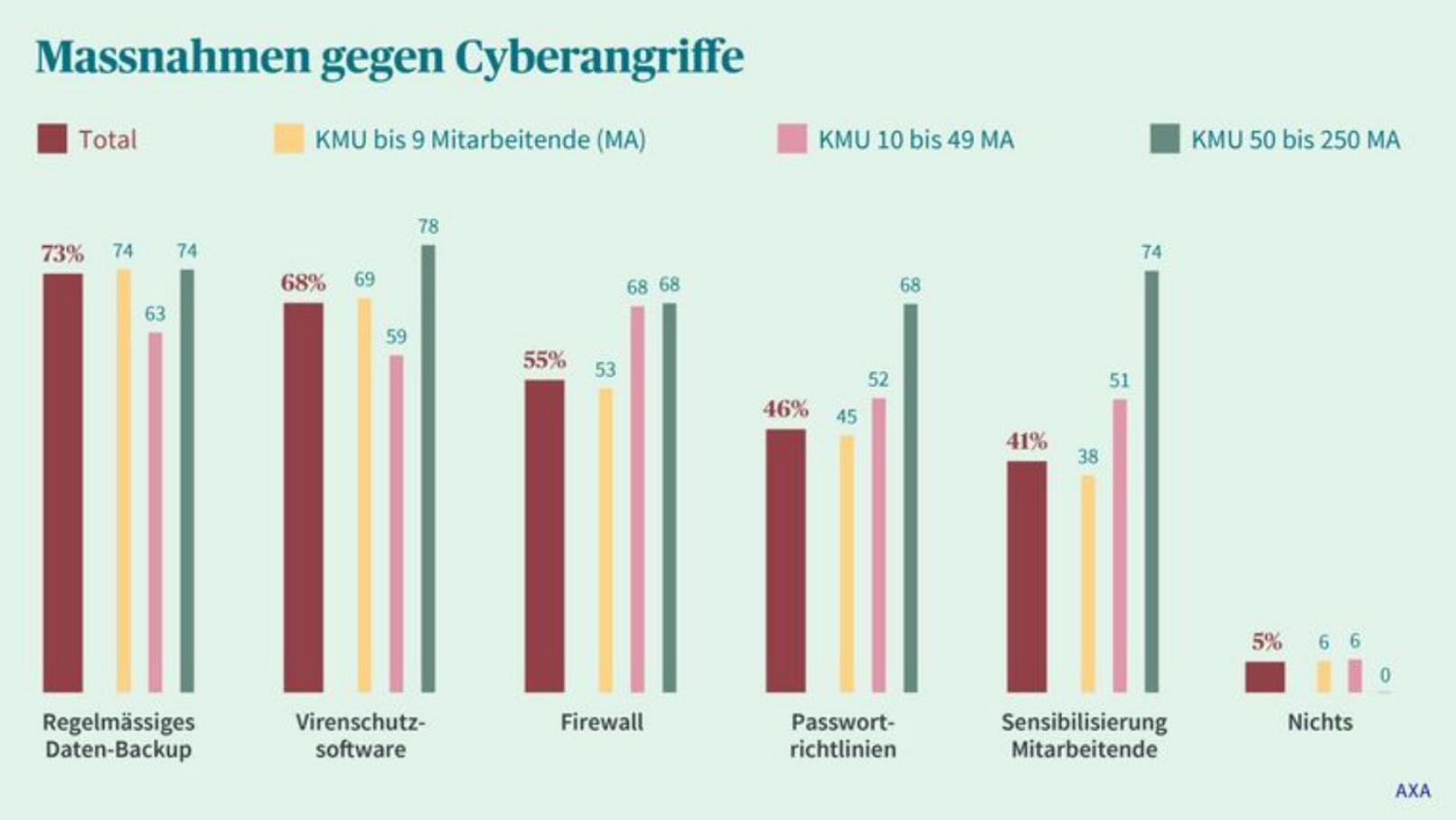
Security Information and Event Management

- Systeme, die Daten im gesamten Netzwerk zentralisieren, korrelieren und analysieren, um Sicherheitsprobleme zu erkennen

Agenda

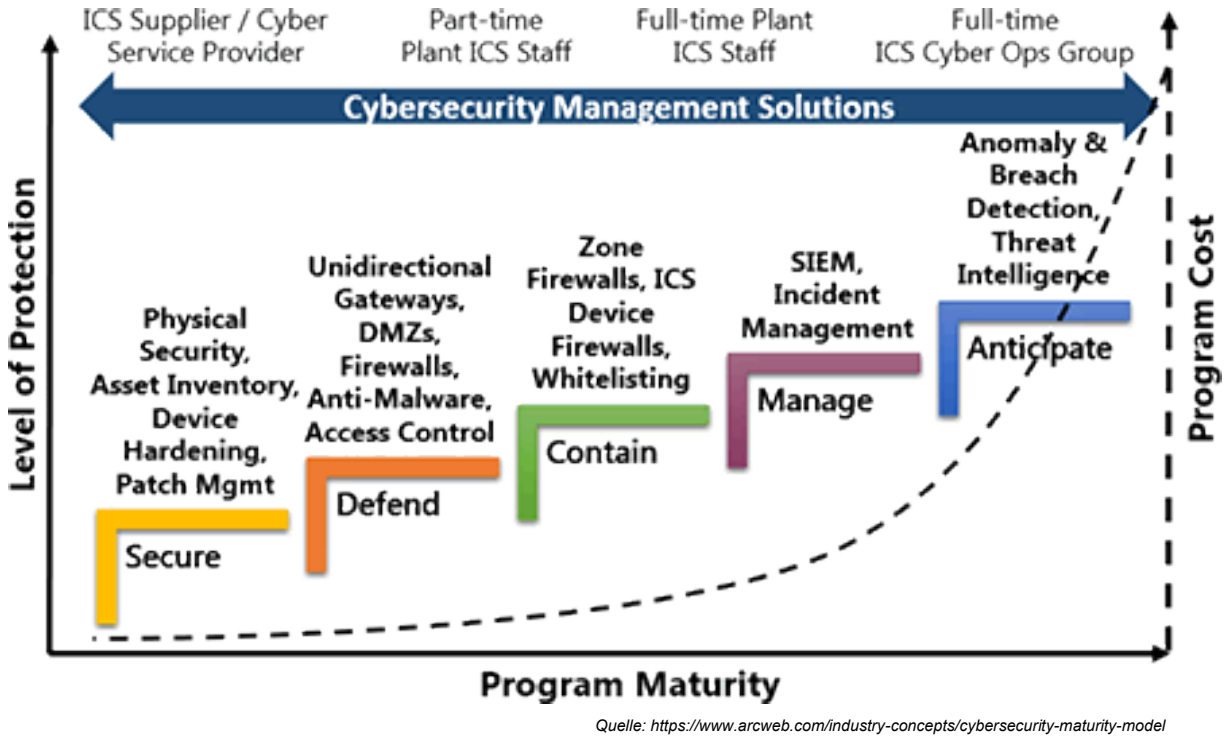
- **Cybersecurity aus Sicht der EKT**
  - als Betreiberin Kritischer Infrastrukturen
  - **als KMU**
- Lösungsangebote von EKT Digital Services unter dem Namen «Protektor Services»

Massnahmen gegen Cyberangriffe in einem typischen KMU



Quelle: https://www.axa.ch/de/ueber-axa/medien/medienmitteilungen/aktuelle-medienmitteilungen/20220830-kmu-studie-digitalisierung-cybersicherheit.html

Cybersecurity aus der Sicht der EKT als KMU



Quelle: https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

Menschen

- Information Security Team (IST) mit Chief Information Security Officer (CISO) in der Organisation etabliert
- Trennung der operativen und strategischen Verantwortung für Informationssicherheit
- Regelmässige Awareness-Massnahmen

Prozesse

- Managementsystem für die Informationssicherheit (ISMS) auf Basis ISO 27001
- Security Operations Center-Prozesse (Detect, Respond, Recover) 7 x 24h durch externe Spezialisten

Technologien

- Firewalls, redundant und zu allen Zonenübergängen
- EDR (Endpoint Detection and Response)
- NDR (Network Detection and Response)
- SIEM (Security Information and Event Mgmt.)
- Zscaler, «VPN always on», gehärtete Endgeräte
- Netzwerkzonierung

Farblegende Massnahmen aus Sicht KMU: umsetzbar, verhältnismässig | Umsetzung nur in begründbaren Fällen | finanziell oder organisatorisch kaum tragbar

Herausforderung Cybersecurity für KMU

Ähnliche Herausforderungen wie Grossunternehmen, aber fehlende Skaleneffekte

Schlüsselfunktionen in KMU müssen sich generalistisch um viele Themen kümmern

Hoher Kostendruck, SOC mit hohem Betriebskostenanteil z.B. schlicht zu teuer

Agenda

- Cybersecurity aus Sicht der EKT
  - als Betreiberin Kritischer Infrastrukturen
  - als KMU
- **Lösungsangebote von EKT Digital Services unter dem Namen «Protektor Services»**

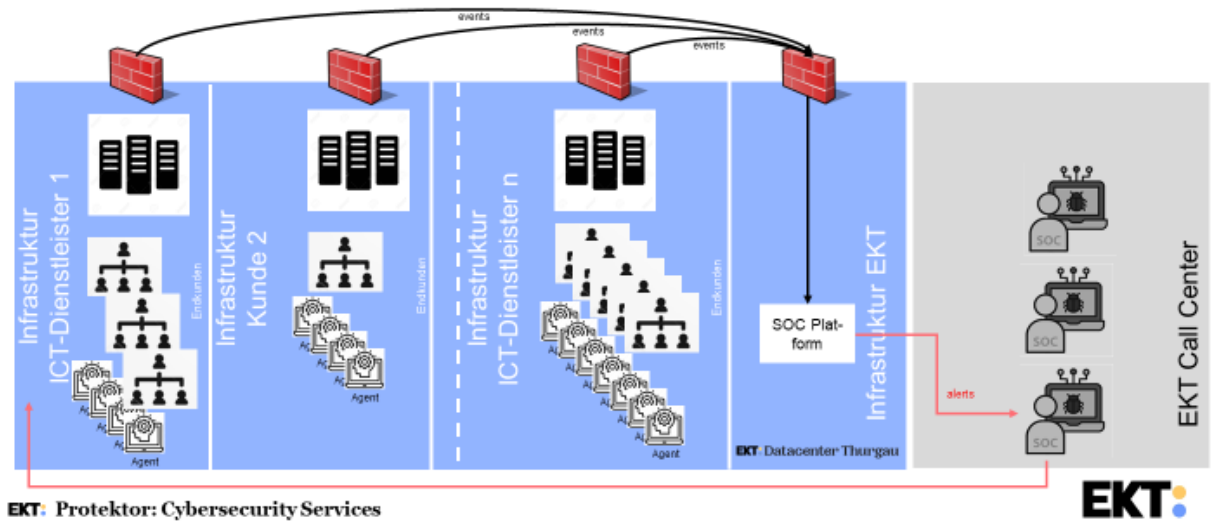
Lösungsansatz EKT für KMU-taugliche Cybersecurity: Protektor Services

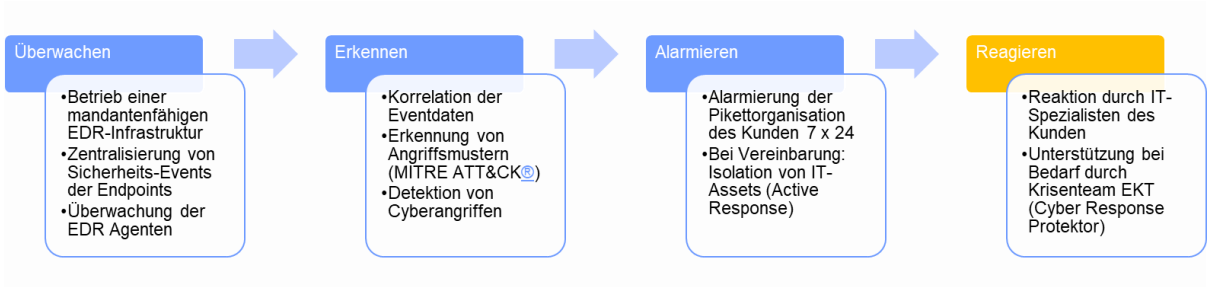
- Die grosse Mehrheit der KMU ist sich der Wichtigkeit der Digitalisierung bewusst und hat in den letzten Jahren technologisch aufgeholt
- Herausforderungen für KMU sind oft fehlendes, spezialisiertes und KMU-taugliches Personal im Cybersecurity-Umfeld sowie für ihre Grösse nicht wirtschaftlich vertretbare Lösungen
- Die EKT als KMU kennt als kritische Infrastrukturbetreiberin beide Aspekte von Cybersecurity, die Seite einer Kritischen Infrastrukturbetreiberin mit umfassenden Schutzmassnahmen, aber auch den Aspekt der beschränkten Ressourcen eines KMU im Markt
- Mit unseren neuen Protektor Services bieten wir unseren Kunden sinnvolle, einsatzerprobte und kostengünstige Lösungen im Umfeld der Cybersicherheit an.

Beispiel 1:
«Cyber Response Protektor»

- Wenn Ihr Unternehmen Opfer einer Cyberattacke wurde, ist eine schnelle Reaktion und professionelle Hilfe entscheidend, um Schäden zu minimieren.
- Für solche Notfälle haben wir unter dem Namen **Cyber Response Protektor** die **EKT: Cyber-Hotline** eingerichtet.
- Unsere krisenerprobten Spezialisten helfen Ihnen **rund um die Uhr, an 365 Tagen im Jahr** schnell und zuverlässig. Damit Sie bei der Krisenbewältigung professionelle Unterstützung bekommen, wenn Sie sie brauchen.
- Mit unserem **Cyber Response Protektor** ist für Sie als EKT Telekom- oder Datacenter-Kunde die **Erstintervention mit Sofortmassnahmen bei einem Vorfall kostenlos**.

Beispiel 2: «SOC Protektor»





- Wer sich nur mit Abwehr schützt, erkennt keine Angriffe: SOC als Lösung zum Aufbau von «Detect»-Fähigkeiten
- EKT Digital Services baut für seine Datacenter-Kunden einen Mehrwertdienst mit dem Namen «SOC Protektor» auf
- «SOC Protektor» ist eine kostenpflichtige Zusatz-dienstleistung, die sich auf das Überwachen, Erkennen und Alarmieren von Cyberangriffen auf die IT-Infrastruktur der Kunden im Datacenter Thurgau konzentriert
- «SOC Protektor» ist für KMU optimiert:
  - Kompetitiver Servicepreis pro Gerät pro Monat
  - 7 x 24 Überwachung und Alarmierung
  - Alarmierung erst bei hoher Wahrscheinlichkeit eines Cyberangriffs
  - Beschränkung auf EDR: 80% aller Angriffe erfolgen über Endpoints
  - Einbindung der IT-Organisation des Kunden im Ereignisfall
  - Ergänzung durch EKT «Cyber Response Protektor» im Bedarfsfall
- Dieser Dienst ist im Aufbau und voraussichtlich ab Juli 2023 für Datacenter Kunden verfügbar!

Fragen

Agenda

- Rückblick
- Referat «Die Cyberpolizei der KAPO TG»
  Selina Märchy, Cybercrime Digitale Forensik, Kantonspolizei Thurgau
  Christoph Gerber, Leiter Cybercrime, Kantonspolizei Thurgau
- Referat «KMU-taugliche Cybersecurity – aus Sicht der EKT»
  Andreas Plüer, Bereichsleiter Digital Services EKT AG
- **Zusammenfassung und Ausblick nächster Anlass**
- Verabschiedung und Ausklang beim Frühstück

EKT: Gipfel Zusammenfassung

- «Big journeys begin with small steps»: sowohl bei der Cyberpolizei der KAPO TG wie auch bei EKT Digital Services mit ihren Cybersecurity-Lösungen unter dem Namen «Protektor Services»
- Die Einheit Cybercrime der KAPO TG erfüllt wichtige Aufgaben bei der Prävention, der Ermittlung, bei der Datenauswertung, der Spurensicherung und der Unterstützung intern wie extern.
- Die Unterstützung und Beratung von Unternehmen im Bereich Cybersecurity gehört aber nicht zum Auftrag der Cyberpolizei
- Das Thema Cybersecurity übersteigt oft die personellen Mittel und das Know-How unserer KMU. Viele der verfügbaren Lösungen liegen zudem ausserhalb der finanziellen Möglichkeiten vieler Unternehmen
- Diese Lücke kann EKT Digital Services mit ihrem neuen Angebot «Protektor Services» schliessen
- Die EKT als KMU kennt als kritische Infrastrukturbetreiberin beide Aspekte von Cybersecurity, die Seite der umfassenden Schutzmassnahmen mit Informationsmanagement-Systeme, aber auch die Möglichkeiten einer KMU
- EKT Digital Services Kunden (Datacenter und Telekom) erhalten in den nächsten Wochen Post: mit der kostenlosen Zusatz-Dienstleistung «Cyber Response Protektor».
- Sprechen Sie uns auf unsere neuen Angebote, insbesondere den SOC Protektor, an!

EKT: Gipfel
Ausblick nächster Anlass

- Save the Date: 27. September 2023, 07.00 Uhr im Gasthaus zum Trauben, Weinfelden

Vielen Dank für Ihren Besuch am EKT: Gipfel

EKT:
Digital Services

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