OST
Ostschweizer
Fachhochschule

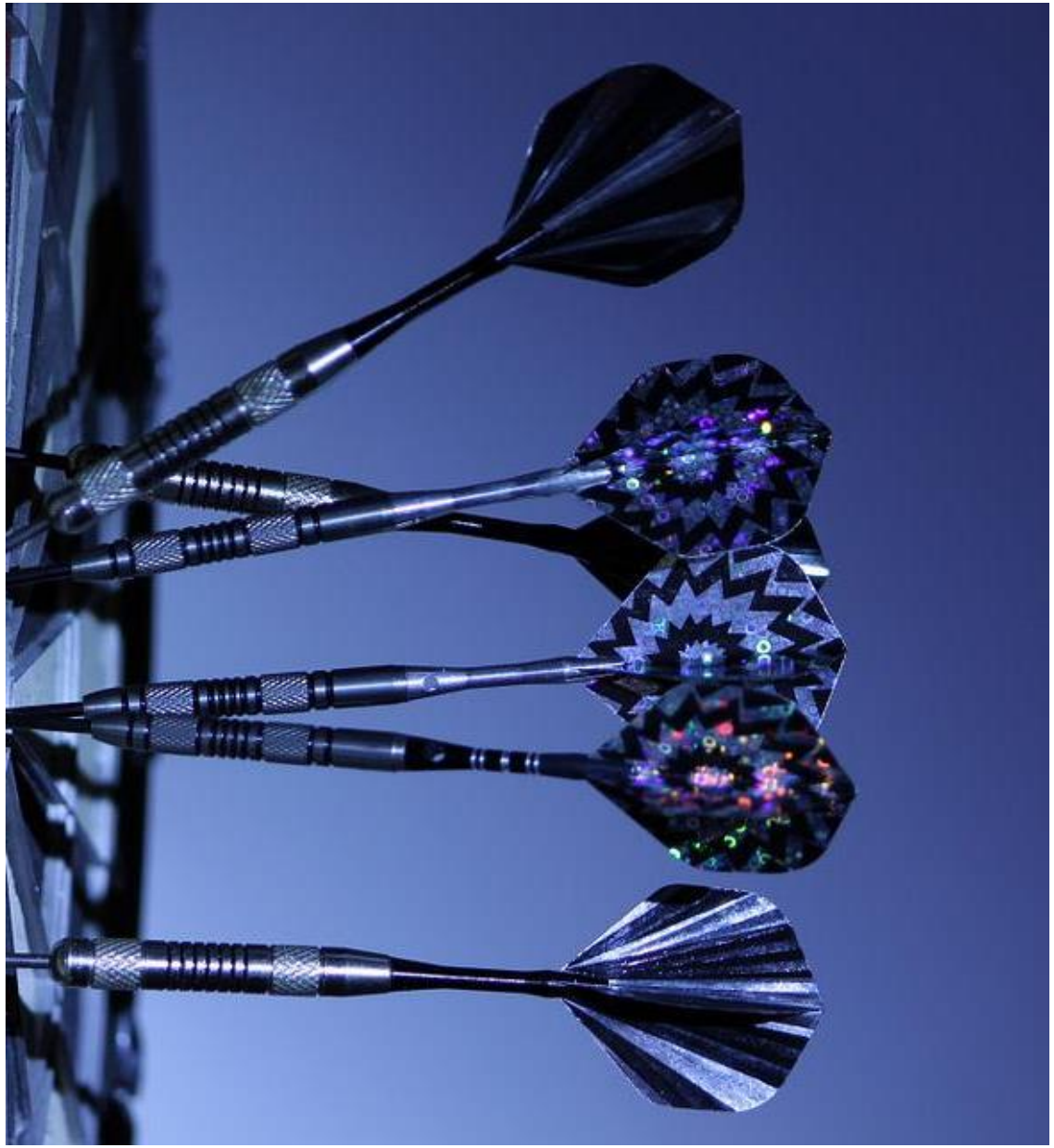
Cyber Security: Kleinvieh macht auch Mist

alumniOST am Campus St.Gallen

Cyber Security: Kleinvieh macht auch Mist

- Aktuelle Bedrohungen
- Warum sind KMU interessante Angriffsziele?
- Wie kann sich ein KMU angemessen vor Cyberangriffen schützen?
- Ich wurde Opfer eines Angriffs – Wie komme ich wieder auf die Füsse?
- Was tut die Schweiz?

Warum sind KMU interessante Angriffziele



KMU nehmen Cybersicherheit zu wenig ernst

- 9 Prozent der Schweizer KMU schützen ihre IT-Arbeitsplätze nicht mit Antiviren-Software
- 15 Prozent schützen ihre Netzwerke nicht mit Firewalls.
- 29 Prozent sichern zwar ihre Daten regelmässig, haben aber nicht getestet, ob sie die Daten überhaupt wiederherstellen können.
- Nur ein Drittel der befragten KMU hat ein Sicherheitskonzept und schult die Mitarbeitenden in IT-Sicherheit, obwohl mehr als 90 Prozent aller Sicherheitsvorfälle auf menschliche Fehler zurückzuführen sind.

- Noch drastischer ist das **mangelnde Bewusstsein** dafür, selbst Opfer eines Cyberangriffes zu werden: Nur gerade 11% schätzen das Risiko, durch einen Cyberangriff einen Tag ausser Gefecht gesetzt zu werden, als gross ein.

OST

KMU als Angriffsziel

- Kleinvieh macht auch Mist: Attacken auf Millionen kleine Unternehmen lohnen sich in der Summe genauso wie ein Angriff auf ein Grossunternehmen.
- Geringer Aufwand (Ransomware as a Service)
- Cyberkriminelle nutzen KMU und deren Daten als Eingangstor, um die IT-Systeme von Grossunternehmen zu hacken.

Ich wurde Opfer eines Angriffs – Wie komme ich wieder auf die Füsse?

Massnahmen nach einem erfolgreichen Angriff

- Im Falle einer Infektion empfehlen wir den Computer sofort von allen Netzwerken zu trennen.
- Danach Neuinstallation des Systems und Ändern aller Passwörter.
- Danach können die Backup-Daten wieder zurückgespielt werden.
- Wenn kein Backup der Daten vorliegt, die verschlüsselten Daten behalten und sichern, damit Sie sie allenfalls später noch entschlüsseln können, sollte hierzu eine Lösung gefunden werden.
- In jedem Falle den Vorfall der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) zur Kenntnis zu bringen und
- Anzeige bei der lokalen Polizeidienststelle zu erstatten.
- Verzichten Sie darauf, ein Lösegeld zu bezahlen. Es gibt es keine Garantie die Schlüssel für die Entschlüsselung zu bekommen

Ich wurde Opfer eines Angriffs - Wie komme ich wieder auf die Füsse?

Erkennen

- System- und Antivirenlogs manuell korrelieren
- Zusammenhänge zwischen einzelnen Vorkommnissen erkennen und analysieren
- ohne SIEM Werkzeuge zum Korrelieren sehr aufwendig

Verstehen

- Datensicherheit gewährleisten
- Backups offline nehmen
- Betroffene Computer sofort vom Netzwerk entfernen
- Lieferanten zur Unterstützung aufbieten
- Weitere Manpower wird benötigt
- Security Spezialisten werden benötigt
- Beziehungen bei Lieferanten und Partner nutzen

Klassifizieren

- Welche Schadsoftware wurde eingefangen?
- Wie hoch ist das Schadenspotenzial?
- Auf welchen Kanälen verbreitet sich die Schadenssoftware?
- Wie weit ist hat sich die Schadsoftware schon verbreitet?
- Handelt es sich um einen mehrstufigen Angriff?
- In welcher Stufe befinden wir uns?
- Welche Mittel und Tools sind für die Eingrenzung notwendig?

Bekämpfen

- Verteidigung
  - Diverse Tools zur Erkennung von Schadsoftware und suspektem Verhalten
  - Manuelle Korrelation von diversen Quellen
  - Ausserbetriebnahme einzelner Systeme
- Angriff – Säuberung
  - Datenkorrelations-werkzeuge implementieren,
  - Automatische Korrelation diverser Systeme
  - Fullscan auf sämtlichen Systemen
    - infizierte Systeme säubern / besser neu installieren
    - Infizierte Userprofiele neu anlegen

OST

Wie kann sich ein KMU angemessen vor Cyberangriffen schützen?

OST

Präventive Massnahmen Ramsomware

- regelmässiges Backup Ihrer Daten. Die Sicherungskopie sollte offline, d.h. auf einem externen Medium sein
- Stellen Sie daher sicher, dass Sie das Medium, auf welche Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer trennen.
- Sowohl Betriebssysteme als auch alle auf den Computern installierte Applikationen müssen konsequent auf den neuesten Stand gebracht werden.
  - Falls vorhanden, am besten mit der automatischen Update-Funktion.
- Vorsicht bei verdächtigen E-Mails, bei E-Mails, welche Sie unerwartet bekommen, oder welche von einem unbekannten Absender stammen.
- Befolgen Sie hier keine Anweisungen, öffnen Sie keinen Anhang, folgen Sie keinen Links.
- Aktueller Virenschutz
- Aktuelle Personal Firewall

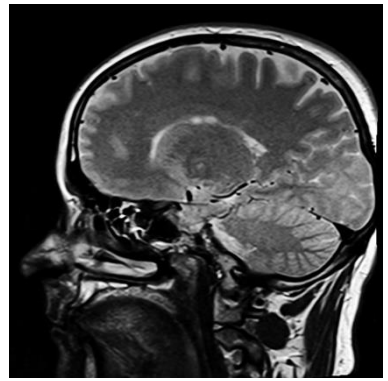
Cybe Security Check: Bin ich gesund?...

Untersuchung Variante 1

Untersuchung Variante 2

Untersuchung Variante 3

Untersuchung Variante 4



Bildquelle: https://pixabay.com/

OST

Methodenbaukasten für Assessments und Checks

Dimension	Gestaltungsoptionen (Kurzbeschreibung)				
Welche Organisationseinheit wird untersucht?	Sparte / Bereich	Abteilung	Behörde		
Wie wird die Untersuchung strukturiert?	Methoden-basiert			Kernfragen-/ Tool-basiert (Schwachstellen)	
	ISO	CS-Basischeck	COBIT, PCI-DSS		
Wie wird untersucht?	Dokumentensichtung	Interviews / Workshops	OnSite-Test		
Wie wird bewertet?	Best Practices (z.B. Standards)	Good Practices (Unternehmensbeispiele)	Benchmarks (Kennzahlen)		
Wie werden die Ergebnisse strukturiert?	Analyse-Ergebnisse		Optimierungs-Maßnahmen		
	Interner Fokus	Vergleichend	Bewertet	Priorisiert	Operationalisiert
Wie werden die Ergebnisse aufbereitet?	Abschlusspräsentation		Abschlussbericht		

OST

Vom Check zu Massnahmenempfehlungem

Ein (umfangreicher, risikoorientierter) Cyber-Sicherheitscheck ermöglicht nachvollziehbare Lösungen und ein einheitliches Verständnis der Sicherheitssituation

Umfang des Checks Flexibilität in der Umsetzung

- Der Scope des Checks ist flexibel. Basis ist z.B. der Check der Cyber-Allianz
- Vor- und Nachteile des jeweiligen Scopes
- Umfang, Dimension und Tiefe sind frei wählbar.

Reifegrad-analyse

Geprüft wird anhand Mindestanforderungen des Basissicherheitschecks Ggf. ergänzt um BSI 100-2 Massnahmen. Dies ergibt den Reifegrad.

Wechselwirkungs- und Risikoanalyse

- Abhängigkeiten und Schnittstellen werden erfasst und analysiert
- Diese Analyse wird den **Risiken** gegenübergestellt und bewertet.

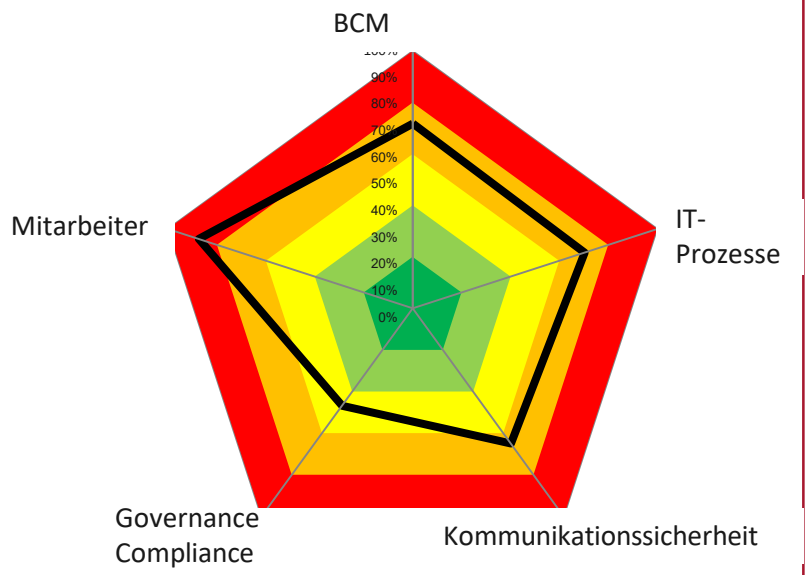
Massnahmenempfehlung

- Massnahmen auf Grundlage des Basissicherheitschecks
- Empfehlungen:
  - Roadmap
  - Bewertete
  - Priorisierung

Risikoanalyse beim Cyber-Sicherheitscheck

Das Risikoprofil wird nach der Reifegradanalyse erstellt, um effektive Massnahmen empfehlen zu können.

Risikoprofil (Bsp.)

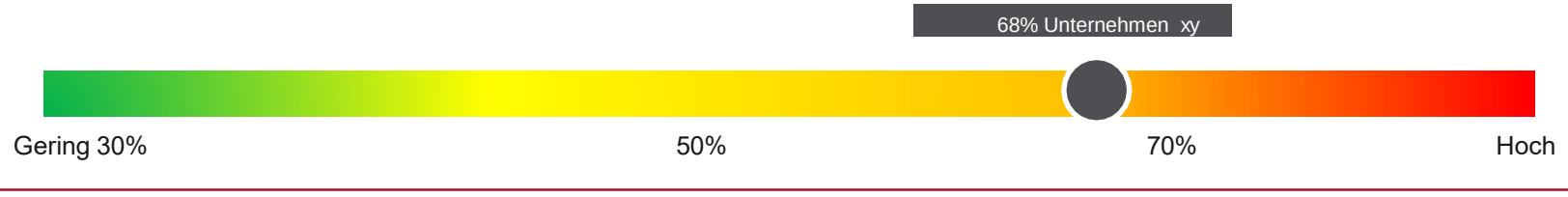


Zusammenfassung

Unternehmen xy sieht sich diversen Gefahren ausgesetzt, die bezogen auf verschiedene Domänen ein Risikoprofil ergeben. In diesem Beispiel hat das Unternehmen ein Risikolevel von 68%.

- Mitarbeiter kennen Cyber-Bedrohungen zu wenig.
- IT-Prozesse sind kritisch aufgrund interner und externer Abhängigkeiten und geeignete Massnahmen für die kritischen Verwaltungsprozesse sind nicht ausreichend etabliert.
- Kommunikationsverbindungen und Authentifizierungsmechanismen sind z.T. ungenügend.
- Compliance ist grösstenteils erreicht, aber nicht gesteuert und gemanagt.
- BCM wird nicht getestet.

Risikolevel



Frau Doktor, bin ich gesund?...vs „gesundes Leben“

Verbesserung der Cybersicherheit UND der Geschäftskontinuität

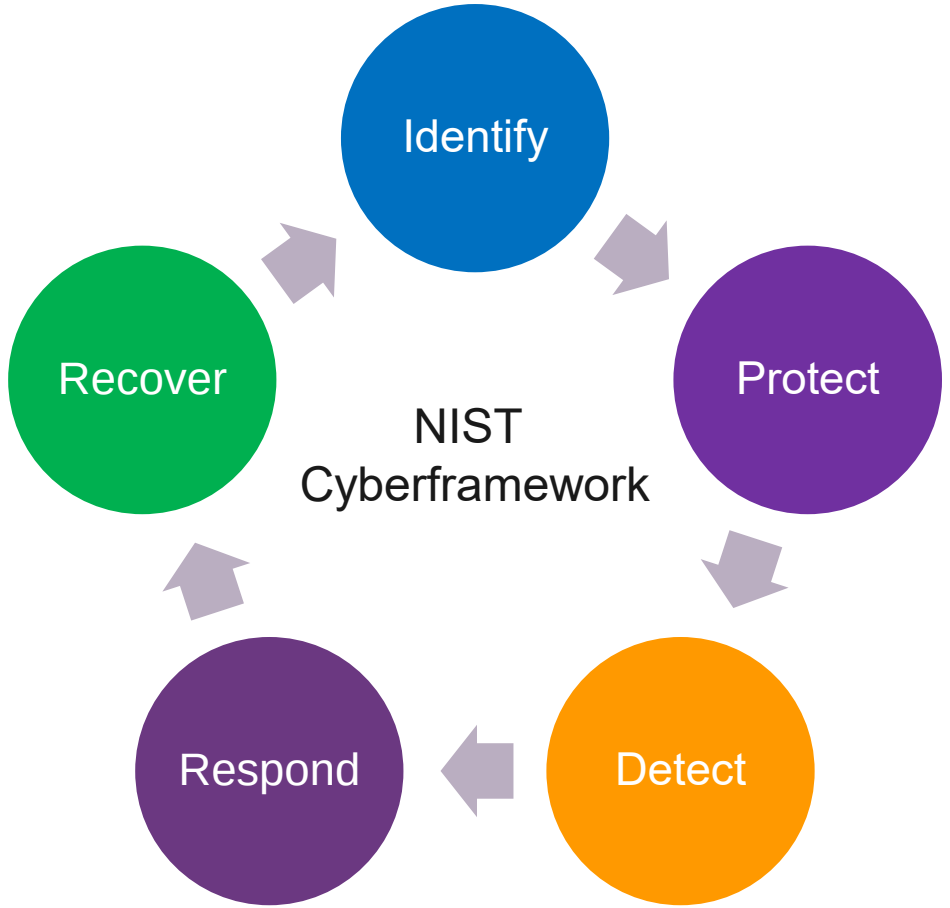
- Ein widerstandsfähiges Unternehmen...
  - verwendet einen ganzheitlichen Ansatz, um die Arbeit zu verstehen/priorisieren und das Risikomanagement in die täglichen Abläufe in ALLEN Geschäftsbereichen zu integrieren
  - weiss, welche Informations- und Kommunikationssysteme unternehmenskritisch sind, und hat Massnahmen ergriffen, um Incidents zu verhindern

OST

Von der Abwehr hin zur Cyberresilienz

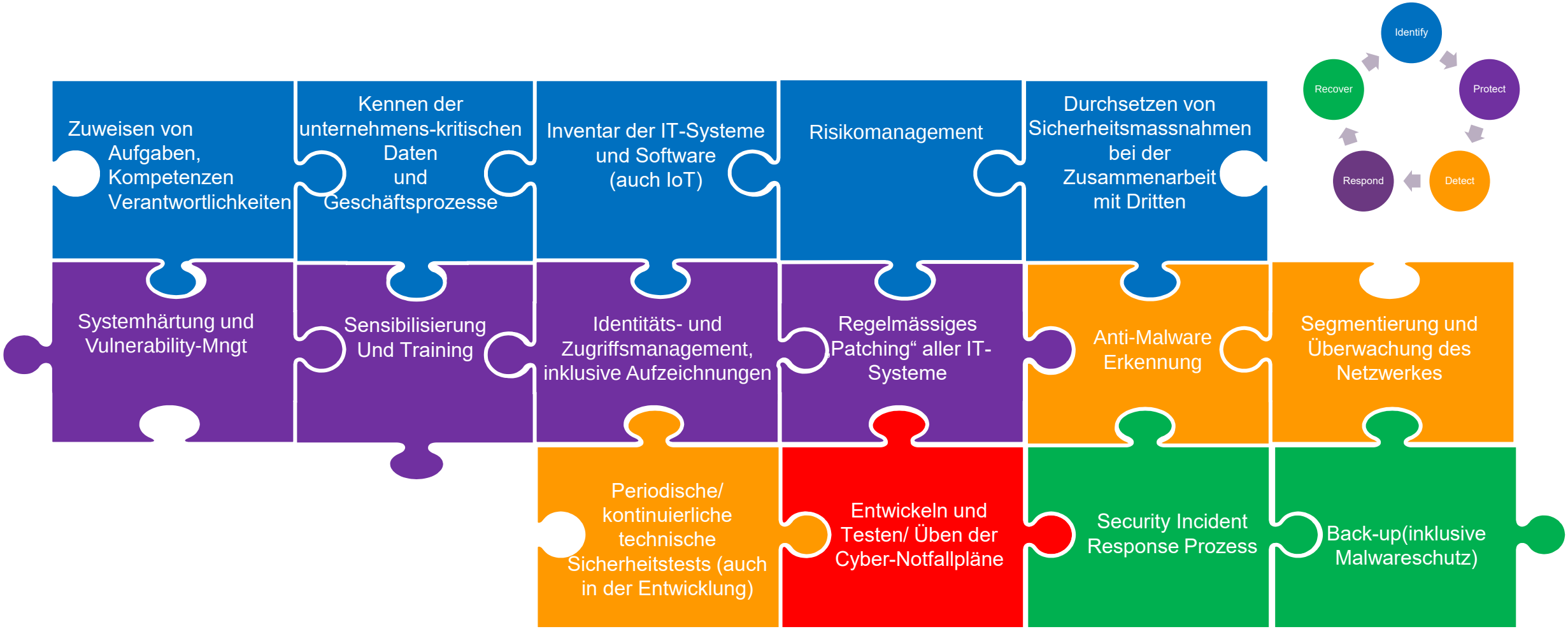
Weg vom. Reinen Fokus auf präventive (meist technische) Schutzmassnahmen

Hin zur verbesserter Detektion und Reaktion



OST

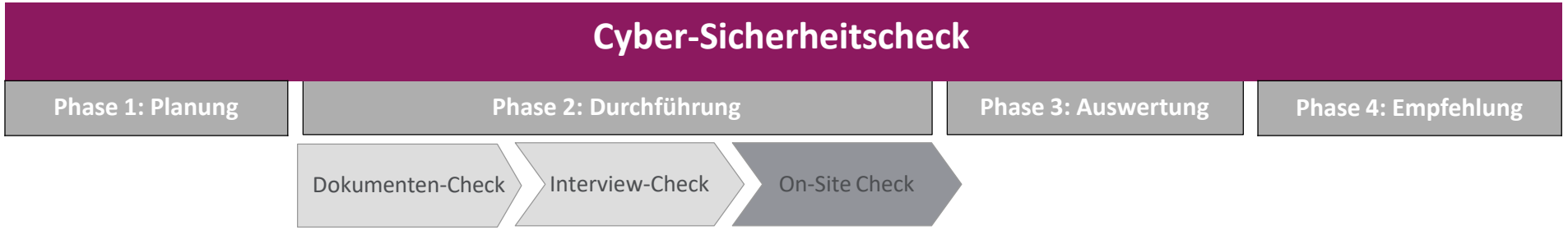
Setzen Sie Grundmassnahmen rigoros um



OST

BACKUP

Horizontale (Vielfalt und Breite) und vertikale (Tiefe der Untersuchungsbereiche) Skalierung.



Bestimmung von:

- Scope
- Ressourcen
- Zeit
- Umfang
- Tools
- …

1. Überprüfung der
   - Organisationsstrukturen zur Cyber-Sicherheit
   - Anwendbarkeit relevanter Regularien
   - Sicherheitsprozesse
   - Security-Produktportfolio
   - IT-Schwachstellen (APT, Botnetz etc.)

   → Feststellung des Reifegrades
2. Ermittlung von Bedrohungen

   → Risikoprofil

3. Technischer Systemcheck (optional mit CP)

Auswertung nach

- Kritikalität
- Wechselwirkung
- Reifegrad
- Priorität

Ergebnisdarstellung

Umsetzungsplanung

Management Summary

Erste Massnahmen zu besser Cyber Security

1. Sichern Sie Ihre Daten regelmässig mit Backups
2. Halten Sie Ihr Antivirus-Programm aktuell
3. Schützen Sie Ihren Internetzugang
4. Aktualisieren Sie Ihre Software regelmässig
5. Verwenden Sie starke Passwörter
6. Schützen Sie Ihre mobilen Geräte
7. Machen Sie Ihre IKT-Benutzerrichtlinien bekannt
8. Schützen Sie die Umgebung Ihrer IKT-Infrastruktur
9. Regeln Sie den Zugriffschutz auf Daten
10. Verschlüsseln Sie mobile Datenträger und Übermittlung
11. Sensibilisieren Sie ihre Mitarbeitenden
12. Regeln Sie die Entsorgung von Informationen und Informationsträgern
13. Überprüfen Sie Ihre Systeme
14. Schützen Sie den Zugang in Ihr Firmennetz durch eine Zwei-Faktor-Authentifizierung
15. Sorgen Sie für eine unterbruchsfreie Stromversorgung
16. Halten Sie wichtige Elemente redundant
17. Planen Sie die Notfallvorsorge
18. Verteilen Sie das Know-How