

AVENIQ

Vom Risiko zur Resilienz – Aveniq's Full-Stack Preventive IT-Security

Ihre heutigen Referenten

Es freut uns, Sie hier begrüßen zu dürfen.



Patrick Gürtler
Senior Strategic Consultant
Aveniq



Werner Stocker
CISO
Aveniq

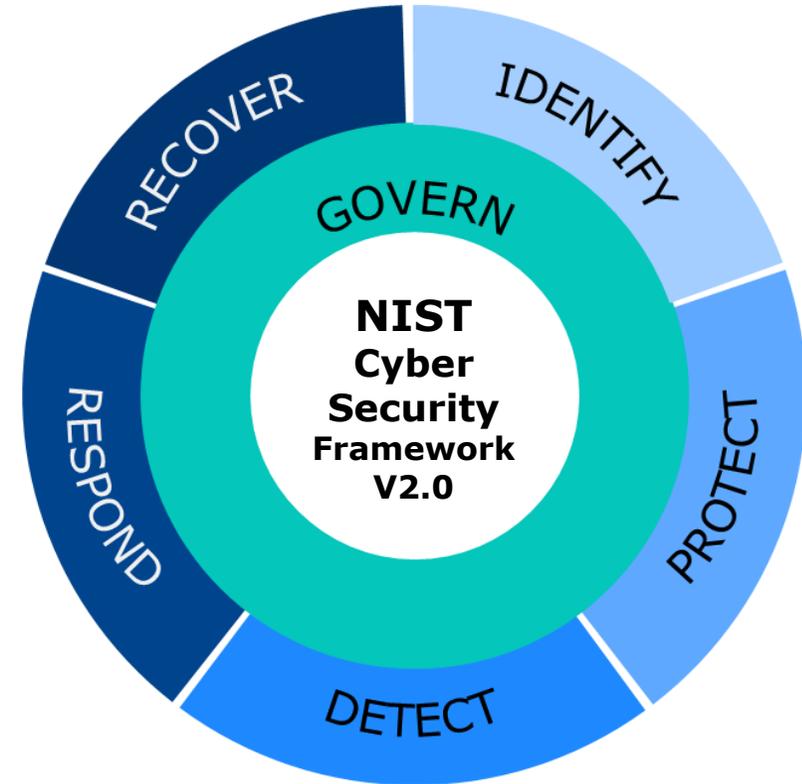
Agenda

NIST2.0-Ausrichtung Produktportfolio

Risikobasierter IT-Grundschutz

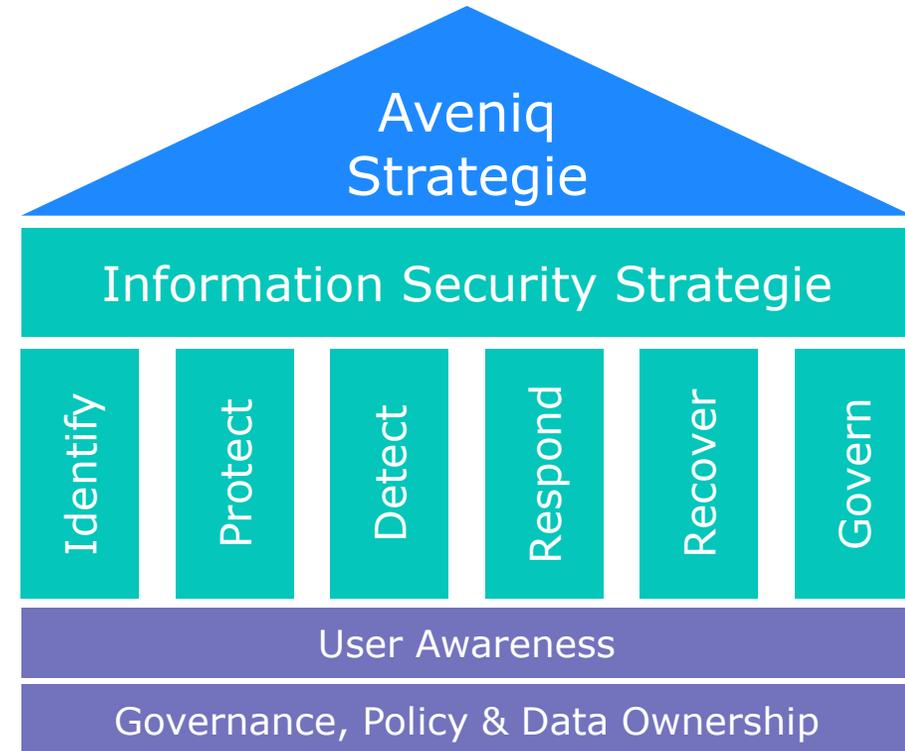
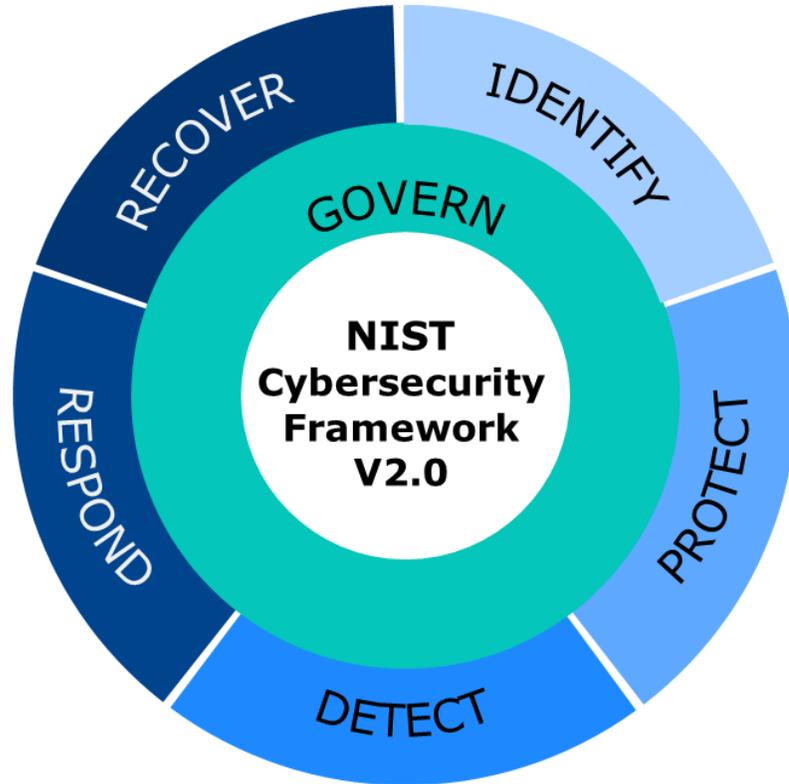


NIST → NIST2.0



NIST 2.0 ist die Basis für unsere Security Services, um eine Full-Stack-Lösung anbieten zu können.

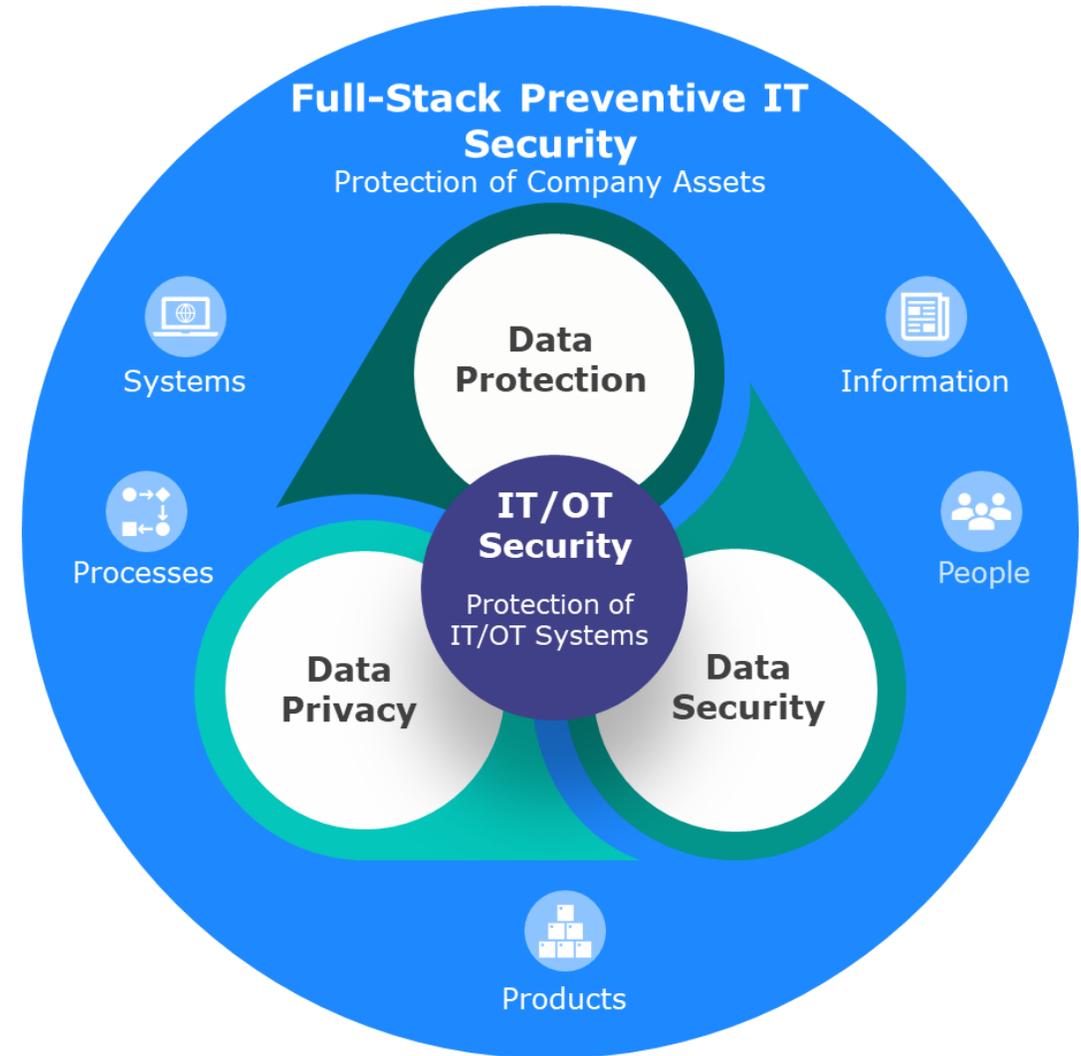
NIST → NIST2.0



Unsere Kund*innen werden häufig von Regulatoren und Auditoren nach NIST geprüft. Sie schätzen sehr, dass wir unsere Services mit dieser Struktur anbieten wollen.

Wir machen sowohl IT als auch OT Security

Daten sind das Herz einer Unternehmung. Die Aveniq-Strategie fokussiert auf Daten und deren Sicherheit. Dies gilt sowohl für IT-Systeme als auch für die in OT zusammengefasste Peripherie.



Zusammen mit unseren Partnern ...

	Identify	Protect	Detect	Respond	Recover	Govern
External Security Service	<ul style="list-style-type: none"> • Avantec • OneConsult • Proofpoint 		<ul style="list-style-type: none"> • Avantec • OneConsult • SecurityScorecard 	<ul style="list-style-type: none"> • Avantec • OneConsult 	<ul style="list-style-type: none"> • Avantec • OneConsult • SecurityScorecard 	<ul style="list-style-type: none"> • Avantec • Fort-IT • OneConsult
Managed Security Service	<ul style="list-style-type: none"> • Microsoft • Palo Alto • SAP • CISCO • Xiting • Tenable 	<ul style="list-style-type: none"> • HPE • Microsoft • Palo Alto • SAP 	<ul style="list-style-type: none"> • Microsoft • Palo Alto • SAP 	<ul style="list-style-type: none"> • Microsoft • Palo Alto 	<ul style="list-style-type: none"> • Microsoft • Palo Alto 	<ul style="list-style-type: none"> • Microsoft • SAP • Proofpoint

Im Managed Service Bereich setzen wir auf drei Kern-Technologiepartner. Für Implementierungen setzen wir auf erfahrene Partner und arbeiten auch eng mit unserer Schwesterfirma Avantec zusammen.

... reduzieren wir unsere Tools von 75 auf < 40

	Identify	Protect	Detect	Respond	Recover	Govern
External Security Service	Analog Mgd. Security Services	Analog Mgd. Security Services	Analog Mgd. Security Services	Analog Mgd. Security Services	Analog Mgd. Security Services	Analog Mgd. Security Services
Managed Security Service	<ul style="list-style-type: none"> • MS Entra ID • MS Purview • MS Defender Vul Mgmt • PA Expanse • CISCO ISE • SAP Identity Management • SAP Code Vulnerability Analyzer • SAP Early Watch Alert • Xiting • EasyBiara • Nessus (Tenable) • Citrix ADC • CheckMK 	<ul style="list-style-type: none"> • MS Intune • MS Advanced Windows Security • MS Defender • MS Purview • PA Strata • PA Prisma • PA Cortex XDR • HPE OneView • HP Connect • SAP Privacy Governance • SAP Data Custodian • UI data protection • SAP Secure Login Service • Xiting • SAP Code Vulnerability Analyzer • Kerberos • Citrix ADC • Citrix Remote Access • HIN SecureMail • Entrust 	<ul style="list-style-type: none"> • MS Defender • PA Cortex XDR • PA Cortex Xpanse • SAP Enterprise Threat Detection • SAP Early Watch Alert 	<ul style="list-style-type: none"> • MS Sentinel • MS Defender • PA Cortex XSOAR • PA Cortex XSIAM 	<ul style="list-style-type: none"> • Windows AutoPilot • PA Crypsis • Veeam 	<ul style="list-style-type: none"> • MS Purview • SAP Security Dashboard • Proofpoint PSAT • EasyBiara

Durch die Fokussierung auf drei Kernpartner für die Tool-Auswahl können wir die Anzahl Tools halbieren.

Agenda

NIST2.0-Ausrichtung Produktportfolio

Risikobasierter IT-Grundschutz



Risikobasierter IT-Grundschutz

Der tägliche Dschungel

**Viele Regulatorien widersprechen sich → Lösungen werden verhindert.
Es kann deshalb notwendig werden Grauzonen in Betracht zu ziehen.**



Cyber Risiken

- Der klassische Perimeter existiert nicht mehr
- Die Angriffslandschaft ist breiter und dynamischer geworden
- Daten sind das neue Gold, auch für Angreifende



Lieferanten

- Wandel zur Cloud
- Sammelsurium an Lieferanten
- Ländergrenzen verschwimmen
- Datenflüsse werden zunehmend komplexer



Regulatorien

- Vielfalt nimmt national und international zu
- Viele sind unübersichtlich und komplex
- Blinde Flecken

Risikobasierter IT-Grundschutz

Herausforderungen Informationssicherheit: Aktuelle Beispiele



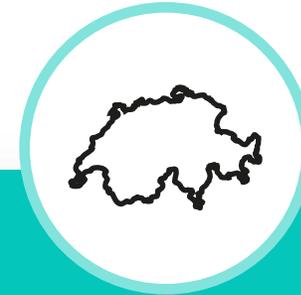
KI

- Angreifer nutzen KI ohne «Gewissen»
- Angriffe sind schneller und professioneller
- Imitationen sind kaum mehr vom Original zu unterscheiden



Microsoft M365

- On-Premise-Dienste werden durch Cloud-Dienste ersetzt - ohne Alternative
- Nicht alle Dienste sind mit Datenhaltung Schweiz erhältlich



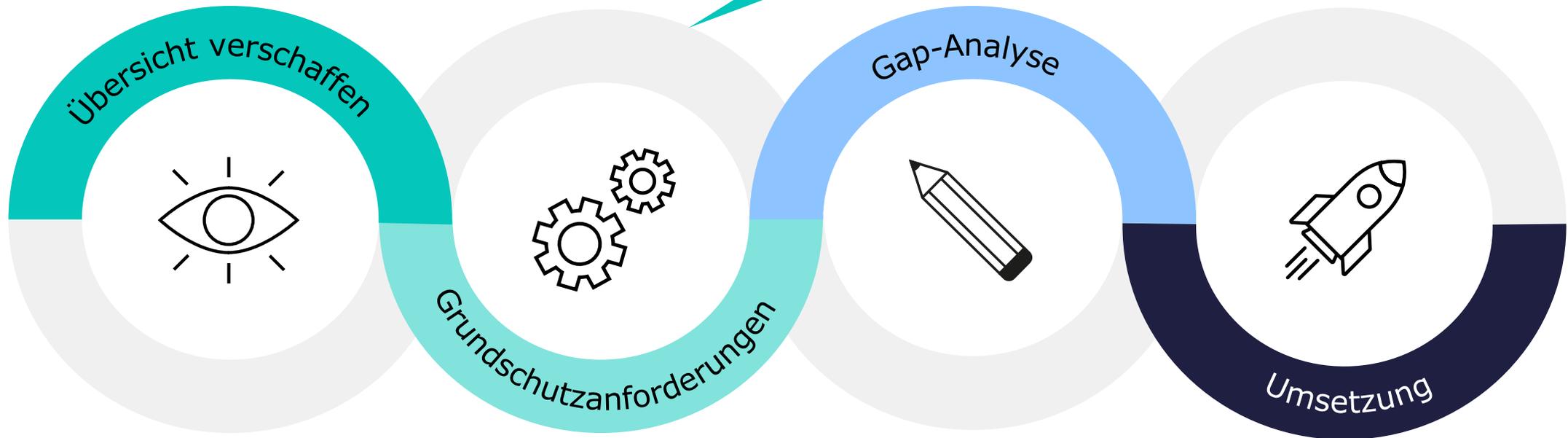
CH DSG vs. EU DSGVO

- Privatbussen CH DSG bis CHF 250'000.-
- Eine Person mit EU/EWR-Bezug erzwingt EU DSGVO
- Inventar versus Liste der Bearbeitungstätigkeiten

Risikobasierter IT-Grundschutz

Sicherheit als Prozess

**Dieser Prozess ist anwendbar
für bestehende sowie neue
Dienstleistungen**



Risikobasierter IT-Grundschutz

Strukturierter Ansatz

DL == Dienstleistung
SB == Schutzbedarf
MN == Massnahmen



Die Herausforderung liegt darin, dies effizient zu strukturieren

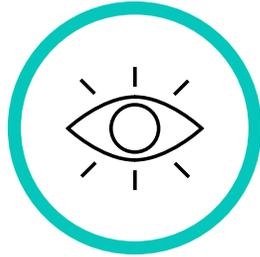
- (1) Angebotene Dienstleistungen identifizieren
- (2) Schutzbedarf Daten und Prozesse festlegen
- (3) Risiken identifizieren
- (4) Schutzmassnahmen definieren
- (5) Schutzmassnahmen umsetzen

Risikobasierter IT-Grundschutz

Aveniq Prozessansatz

Liefert auch Grundlage für Lieferantenmanagement

Jährliche Wiederholung stellt Aktualität sicher



In einem zentralen Register werden die Dienstleistungen mit Schutzbedarf und Regulatorienbindung dokumentiert.

Ein regelmässiger Review ergänzt das Inventar und trägt Veränderungen nach.

Basierend auf dem Schutzbedarfsniveau und den gebundenen Regulatorien werden Risiken mit einem standardisierten IT-Grundschutz bewertet.

Zum IT-Grundschutz abweichende Risiken werden über Massnahmen behoben oder vom Datenbesitzer als Restrisiko getragen.

Bei wesentlichen Veränderungen in den Dienstleistungen oder Regulatorien, können über das Inventar Risiken proaktiv gemanagt werden.

Chancen

Risikobasierter IT-Grundschutz



Mit Ihnen auf Augenhöhe

Aveniq hat ein besseres Verständnis für Sie – auch betreffend Branche und Geschäftsmodell.

Aveniq erbringt Leistungen punktgenau auf Ihre Bedürfnisse abgestimmt.



Nachhaltige Sicherheit

Bei Risiko-Abweichungen kommt Aveniq regelmässig und proaktiv auf Sie zu und erarbeitet mit Ihnen wo nötig Zusatzmassnahmen.

Sie entscheiden selbst über Ihren eigenen Risikoappetit. Tritt ein Risiko ein, so ist dokumentiert, warum es von Ihnen akzeptiert wurde.



Vollständigkeit

Aveniq zeigt sich im Markt als Provider, der proaktiv Governance und Compliance individuell auf Kunden abstimmt und aufgrund der Standardisierung zu fairen Preisen anbietet.

Mit der Ausrichtung auf NIST2.0 und Zero Trust wird gleichzeitig auch die Vollständigkeit sichergestellt.

AVENIQ

Und wo stehen Sie?

Wie und wo kann Aveniq
Sie unterstützen?

AVENIQ

Haben Sie Feedback für uns?

Herzlichen Dank

