Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023

Webinar:
Security für mittelständische Firmen

Christian Grob
Head of Security Services, grob@avantec.ch

Agenda

1. Update Bedrohungslage
2. Herausforderungen
3. Exponierung für Cyber Angriffe
4. Cyber Sicherheitsdispositiv (Blueprint)
5. Typische GAPs im Dispositiv
6. Bewältigungsstrategie
7. Threat Detection Komponenten
8. AVANTEC CDC / MDR Module
9. Mehrwert unserer Cyber Defense Services
10. Q&A

Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023

Update Cyber Bedrohungslage

AVANTEC
Competence. Security. Trust.

435 Meldungen im H1 2023 zu Hacking & Schadsoftware beim Nationalen Zentrum für Cyber Sicherheit (NCSC)

Terabytes sensitiver Daten von CH Unternehmen **im Dark Web** – Double Extortion beliebt bei Angreifer

Cyberkriminelle werden **professioneller** – **84 Minuten** vergehen gemäss CrowdStrike vom Initial Access -> Lateral Movement

Ungepatchete **Schwachstellen**, offene oder **falsch konfigurierte** extern erreichbare Dienste, **Supply-Chain Angriffe**

Das **Zeitfenster**, um Angriffe abzuwehren bevor diese einen grösseren Schaden anrichten, **wird immer kleiner**

Mittelständische Unternehmen vermehrt im Visier, **fehlende Ressourcen** im Bereich Cyber Sicherheit führen zu Breaches

www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html
www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023/

Herausforderungen

AVANTEC
Competence. Security. Trust.

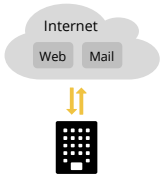
AVANTEC
Competence. Security. Trust.

Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023

Exponierung für Cyber Angriffe

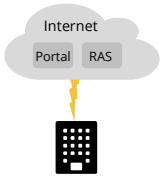
AVANTEC
Competence. Security. Trust.

Internet & E-Mail — A



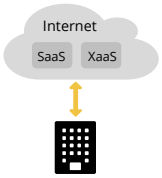
Gefährdungen
- Phishing Mails (Attachments, Links)
- Drive-by Infektionen (Client seitige Schwachstellen)
- Download maliziöser Dateien
- (Office Dokumente, PDF, Executables)

Exponierte Dienste im Internet — B



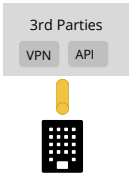
Gefährdungen
- Schwachstellen in externen Diensten (Software Bug, Fehlkonfigurationen) in Websites/Webserver/DB
- Schwachstellen oder missbrauch von Accounts in Remote Access Services (VPN, Citrix)

Cloud basierte Dienste — C



Gefährdungen
- Schwachstellen in externen Diensten (Software Bug, Fehlkonfigurationen) in Cloud Services XaaS
- Schwache Einstellungen im Bereich Identity & Access Management - missbrauch von Cloud Accounts

Lieferanten & Drittanbieter — D



Gefährdungen
- Angriffe über vermeintlich vertrauenswürdige Dritte – Verbindungen oft weniger gut geschützt
- Verbreitung von Ransomware über etablierte Verbindungen
- Manipulierte Produkte, Tools, System Images in der Lieferkette

Cyber Sicherheitsdispositiv - Blueprint

AVANTEC
Competence. Security. Trust.

Security Policies | **Roles & Responsibilities** | **Security Architecture** | **BC & DR Planning** | **Change Control** | **Configuration Mgmt**

Vulnerability Management
- Externe/Interne Vulnerability Scans
- Proaktives (autom.) Patch/Lifecycle Mgmt
- Aktive Überwachung der Behebung inkl. Eskalationsprozess

Secure Configuration
- Sichere Konfiguration der Systeme (CIS Benchmarks)
- Deaktivierung von Default Accounts, nicht benötigen Diensten, schwache Protokolle

Access Control
- 2FA (min.) auf ext. Applikationen, Remote Access & privilegierten Benutzern
- Restriktive/dedizierte Admin Accounts (PAM)
- Zentrales IAM/RBAC

Penetration Testing
- Periodische externe (gesamte Angriffsfläche) & interne Pentest (kritische Systeme)
- Aktive Überwachung der Behebung inkl. Eskalationsprozess

Web & Mail Protection
- Kontinuerliche Updates aller Komponenten (Browser, Office)
- Anti-Phishing/Spam Erkennung
- Web Proxy/Filtering
- Sandboxing

Secure Backup & Recovery
- Automatische Sicherung der Daten/Systeme
- Schutz vor Löschung, Verschlüsselung mittels «immutable/offline» Speicherung
- Test Wiederherstellung

Endpoint Protection
- Moderne EPP
  - Verhaltensbasierte Erkennung (IOA)
  - Integrierte Theat Intelligence (IOC)
  - Zentrales Mgmt
- App Whitelisting

Application & Network Security
- Schutz von Web Apps mit WAF/Proxy
- Blockierung auffälliger Netzwerkverkehr - IPS
- Firewall - Netzwerk Zonierung
- Micro Segmentierung

Detection & Response
- State-of-the Art Threat Detection (Security Analytics, XDR/EDR/NDR)
- 24/7 Security Monitoring & Security Incident Response (MDR)
- Zentrale Log Speicherung

Data Protection
- Verschlüsselung sensitiver Daten
  - beim Transport (TLS, SSH, IPSEC)
  - bei der Speicherung je nach Use Case File, App, DB, Storage

IT Asset Mgmt | **Audits & Reviews** | **Security Awareness** | **3rd Party Risk Mgmt** | **Threat Monitoring** | **Cyber Crisis Mgmt**

AVANTEC
Competence. Security. Trust.

Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023

Typische GAPs im Dispositiv

AVANTEC
Competence. Security. Trust.

Security Policies	Roles & Responsibilities	Security Architecture	BC & DR Planning	Change Control	Configuration Mgmt

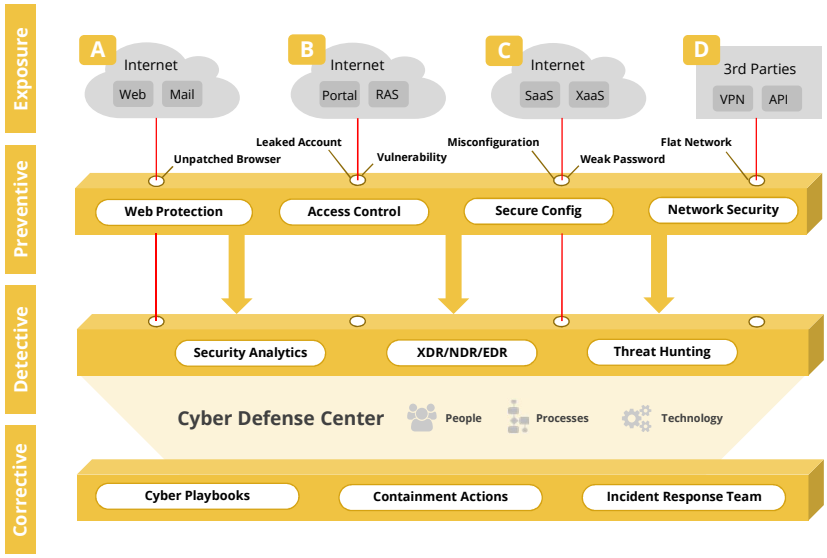
Vulnerability Management	Secure Configuration	Access Control	Penetration Testing	Web & Mail Protection
▪ Ungenügende Scan Coverage ▪ Patches wären seit Monaten verfügbar ▪ Ignoranz von Vuln. ohne Patch ▪ SW/HW Out of Support ▪ Ineffektives Tracking	▪ Keine Vorgaben für sichere Konfiguration -> Wildwuchs ▪ Fehlende automatisierte Überprüfung der Einstellungen ▪ Unnötige Exponierung	▪ Username/PW für externe Dienste & privilegierte Benutzer ▪ Vermischung von User/Admin Rechten ▪ Zu viele Admins ▪ Dezentrale Vergabe von Rechten	▪ Verwechslung mit Vuln. Scanning ▪ Nur unauthentisierte Tests ▪ Fehlende Test vor Go-Live neuer Apps, Infra, Systeme ▪ Keine Re-Tests	▪ Alle möglichen Browser im Einsatz -> mit Schwachstellen ▪ Minderwertige Spam Erkennung mit zu hohen Durchlassraten ▪ Web/Mail Kanal ohne Threat Protection

Secure Backup & Recovery	Endpoint Protection	Application & Network Security	Detection & Response	Data Protection
▪ Backups werden nicht getestet ▪ Undokumentierte Abläufe für die Wiederherstellung ▪ Backupsysteme sind im LAN -> teilweise in «flachen Netzen»	▪ Einsatz von Legacy AV Software die Primär auf Signaturen basiert ▪ Kein EDR im Einsatz ▪ Fehlende zentrale Sicht ▪ Benutzer können selber Applikationen installieren/ausführen	▪ Web Apps direkt im Internet, keine Überprüfung des Datenverkehrs mit WAF, Input Validation ▪ Flache Netzwerke -> Any Rules , kein Zonenkonzept	▪ Fehlende Threat Detection ▪ Technologien teils vorhanden aber kein (qualifiziertes) Personal für Analyse & Response ▪ Nur Bürozeiten	▪ Unverschlüsselte Übermittlung sensitiver Daten, inkl. Authentisierungsdaten ▪ Schwache Algorithmen Protokolle/Key Längen ▪ Ungenügend geschützte Keys

IT Asset Mgmt	Audits & Reviews	Security Awareness	3rd Party Risk Mgmt	Threat Monitoring	Cyber Crisis Mgmt

Bewältigungsstrategie

AVANTEC
Competence. Security. Trust.



1) Es ist davon auszugehen, dass Angreifer vorhandene Schwachstellen ausnutzen
2) Neben präventiven Massnahmen sind detektive Massnahmen unerlässlich
3) Gezielter Einsatz von externen Cyber Defense Services, um interne Lücken zu schliessen

AVANTEC
Competence. Security. Trust.

Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023

Threat Detection Komponenten

AVANTEC
Competence. Security. Trust.

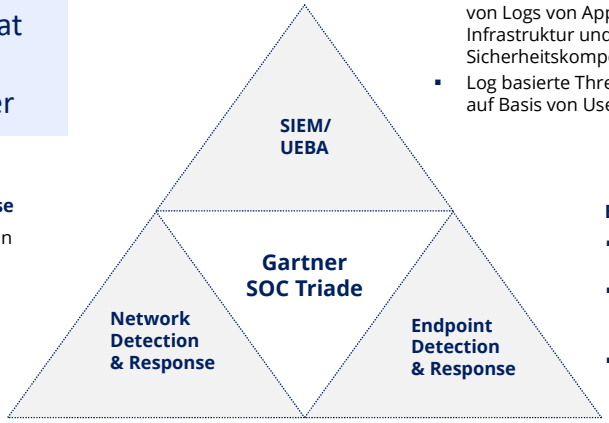
"No organization can stay safe without foundational threat detection and response." Gartner

Security Information & Event Mgmt

- SIEM/UEBA ermöglicht das Sammeln und Analysieren von Logs von Applikationen, Infrastruktur und Sicherheitskomponenten.
- Log basierte Threat Detection auf Basis von Use Cases

Network Detection & Response

- Erkennung von Bedrohungen im Netzwerk durch die Überwachung des Netzwerkverkehrs
- Kombination verschiedener Analyse-Verfahren
- Keine Installation von Software auf Systemen



Endpoint Detection & Response

- Erkennung von Bedrohungen auf dem Endpoint
- Ermöglicht mit umfangreicher Telemetrie das Verhalten des Angreifers nachzuvollziehen
- Eingriffe auf den Systemen wie z.B. die Isolation möglich

Source: Gartner, Applying Network-Centric Approaches for Threat Detection and Response
ID G0037346

AVANTEC CDC / MDR Module

AVANTEC
Competence. Security. Trust.

Modularer Aufbau der Services ermöglicht individuelle Zusammenstellung

Schrittweiser Ausbau zur Steigerung der Maturität und kontinuierlichen Anpassung an die Bedrohungslandschaft

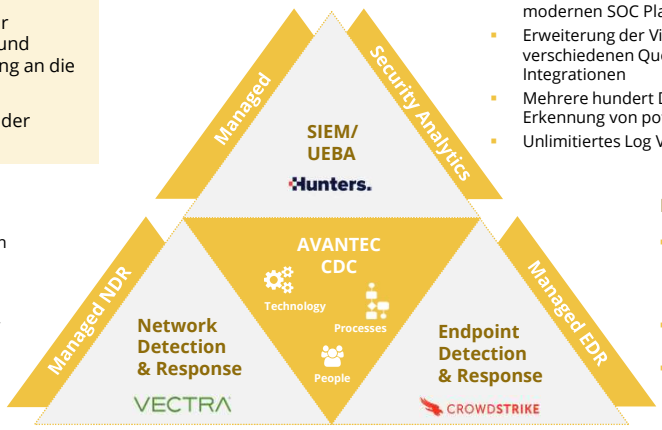
Technologie wird als Teil der Services **bereitgestellt**

Managed Security Analytics

- Korrelation und Analyse von sicherheitsrelevanten Daten auf Basis der modernen SOC Plattform von Hunters
- Erweiterung der Visibilität mit Daten aus verschiedenen Quellen – Umfangreiche Integrationen
- Mehrere hundert Detectors für zuverlässige Erkennung von potenziellen Cyber-Angriffen
- Unlimitiertes Log Volumen

Managed NDR

- Überwachung des gesamten Netzwerkverkehrs mit der innovativen Technologie von Vectra
- Kombination verschiedener Analyse-Verfahren (u.a. Machine Learning/AI)
- Ohne Agent auf den Endpoints



Managed EDR

- Überwachung der Client und Server mittels Endpoint Sensor & cloud-basierter Management Technologie von CrowdStrike
- Next GEN AV, EDR und Threat Hunting inklusive
- Umfangreiche Handlungsoptionen und direkter Eingriff auf Endpoints bei Alerts

Source: Gartner, Applying Network-Centric Approaches for Threat Detection and Response
ID G0037346

AVANTEC
Competence. Security. Trust.

Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023

Mehrwert unserer Cyber Defense Services

AVANTEC
Competence. Security. Trust.

Service Inbetriebnahme
- Erfahrenes Team leitet durch das Onboarding
- Vorkonfiguration der eingesetzten Technologie nach Best Practices
- Rollout in kürzester Zeit

Security Monitoring
- Analyse & Triage der Security Events gemäss definierten SLA
- Tiefergehende Security Investigation - rund um die Uhr 24/7

Incident Response
- Standard Playbooks werden auf Kunden angepasst
- Sofortige Einleitung von Eindämmungsmassnahmen gemäss Playbooks (z.B. Isolation von Endpoints)

Modernste Technologie
- State-of-the-Art Threat Detection der führenden Anbieter inklusive
- Module optimal aufeinander abgestimmt, integriert & konfiguriert

Kostentransparenz
- Hohe Kostentransparenz & Planbarkeit durch pauschale Preise – Endpoint basiert
- Attraktive Preise durch MSSP Skalierungseffekt

Zertifizierte Experten
- Zugriff auf zertifizierte Experten (u.a. GIAC Certified Forensic Analyst (GCFA), GIAC Continuous Monitoring (GMON)
- 24/7 Telefonnummer

AVANTEC
Competence. Security. Trust.

DANKE
> Q&A

AVANTEC
Competence. Security. Trust.

AVANTEC
Competence. Security. Trust.

Backup Slides

MDR Service Übersicht

AVANTEC
Competence. Security. Trust.

Detection
Erkennung von abnormalem und maliziösem Verhalten auf Basis State-of-the Art **NDR und EDR Technologie**
Automatisierte Eröffnung eines Cases bei AVANTEC

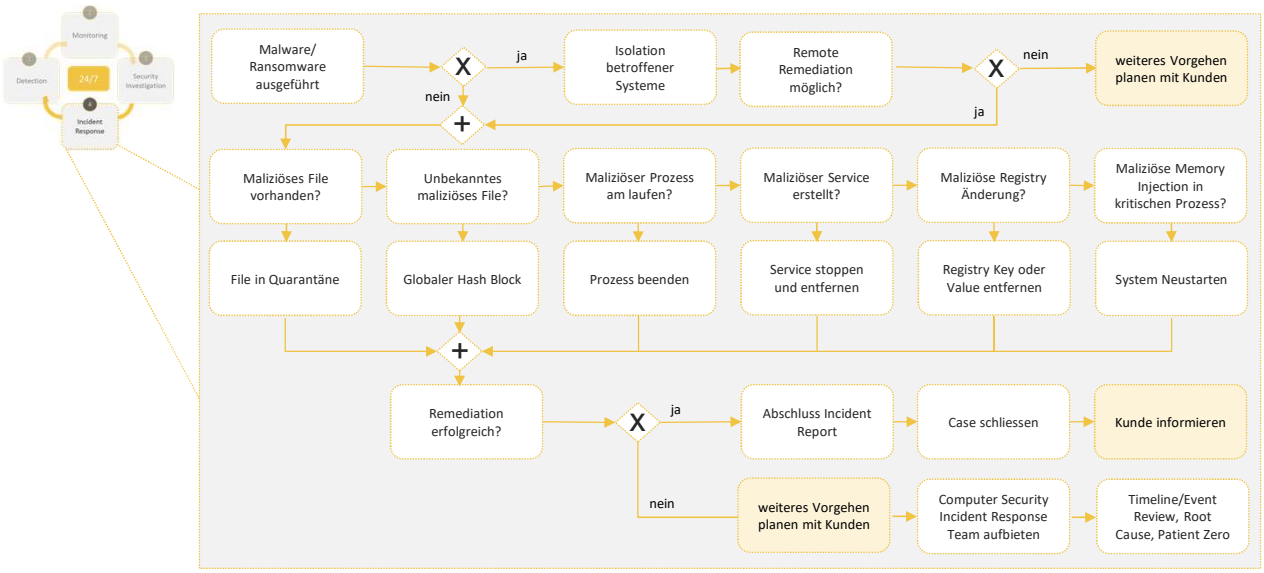
Monitoring
Erstanalyse der generierten Security Events durch MDR Analysten und ggf. **Triage für weitere Investigation**
Automatisierte Response möglich

Security Investigation
Durchführung **tiefergehende Analyse** unter Einbezug von weiterem Kontext (Asset Information, Threat Intelligence, System Artefakten etc.)
Information an MDR Kunde bei Security Incident
Eskalation Incident Response Team (AVANTEC / Kunde)

Incident Response
Massnahmen werden in enger Zusammenarbeit mit dem Kunden gemäss definiertem **Szenario (Playbook)** ausgeführt sowie die **Recovery** begleitet
Abschluss Incident Report & lessons learned

AVANTEC
Competence. Security. Trust.

Incident Handling & Remediation



Einsatz von Automatisierung

Wir setzen stark auf Automatisierung mit dem Ziel:

- Möglichst rasch auf eine Bedrohung zu reagieren (fast response)
- Einen Ausbruch einzudämmen (outbreak mitigation)
- Datenabfluss zu verhindern (data loss mitigation)
- Den Service mit Best-Of-Breed Detection & Response Technologie kosteneffizient zu erbringen (Efficiency)

Fast response	Outbreak mitigation	Data loss mitigation	Efficiency
▪ Isolation des Hosts mittels EDR ▪ AVANTEC SOAR (z.B. Verschiebung in anderes VLAN)	▪ Blockierung des Zugriffs (z.B. IP, URL) des Absendersystems oder Zielsystems ▪ Blacklisting eines Files (File Hash)	▪ Deaktivierung des Accounts im Active Directory ▪ Limitierung des Zugriffs (z.B. Entzug Berechtigung)	▪ Automatisierte Sandbox Scans ▪ Automatisierte Prüfung und Anreicherung Threat Intelligence (z.B. Abfrage IOC)

Standard MDR SLA

AVANTEC
Competence. Security. Trust.

24/7 Response Times - Acknowledgement

Detection & Response	Critical	High	Medium	Low
Business hours 08:00-18:00	1h	2h	Next Business Day	Best Effort
Off hours Mo-Fr 18:00-08:00 Sa-So 00:00-00:00	1h	2h	Next Business Day	Best Effort

Vorgehen Onboarding

AVANTEC
Competence. Security. Trust.

Prework

- Abklärung
  - Requirements
  - Scope
  - SLA
  - Responsibility Model
- Teststellung (bei Bedarf)

Contracting

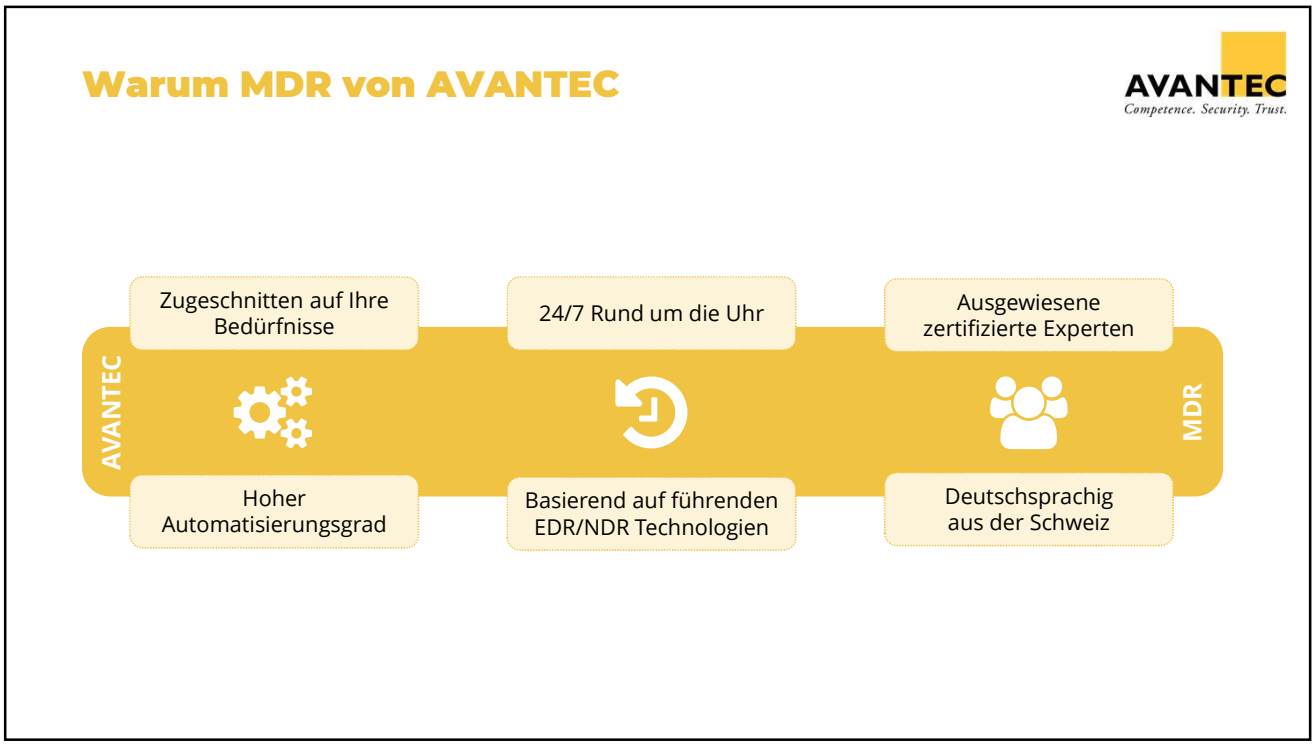
- Vertrag erstellen
  - Service Beschreibung
  - SLA
  - Responsibility Model
  - Governance
  - Abhängigkeiten
  - Vertrag Sign-off und Kick-off

Onboarding

- Gemeinsame Rollout Planung
- Erstellen der Architektur
- Erstellen der Playbooks
- Konfiguration der Systeme & Rulesets
- Pilotierung (ggf. in Iterationen)
- Produktiver Rollout
- Schulung

AVANTEC
Competence. Security. Trust.

Webinar: Security für mittelständische Unternehmen
31. August / 6. September 2023



AVANTEC
Competence. Security. Trust.