Zscaler Business Update
05. März 2024

Cyber Defense/MDR – Zscaler Event

Christian Grob
Head of Security Services
grob@avantec.ch

Agenda

1. Update Cyber Bedrohungslage
2. Exponierung für Cyber Angriffe
3. Herausforderungen
4. Bewältigungsstrategie
5. Threat Detection Komponenten
6. AVANTEC CDC / MDR Module
7. Fazit und Empfehlungen

Zscaler Business Update
05. März 2024

Cyber Bedrohungslage

AVANTEC
Competence. Security. Trust.

Knapp 50'000 Meldungen im 2023 beim Nationalen Zentrum für Cyber Sicherheit (NCSC) – im Vergleich zum Vorjahr +30%

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

Cyberkriminelle werden **professioneller** – **64 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-2024/

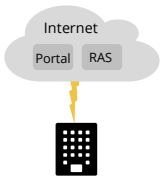
Exponierung für Cyber Angriffe

AVANTEC
Competence. Security. Trust.

Internet & E-Mail A

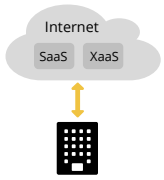
Gefährdungen
- Phishing Mails (Attachments, Links)
- Drive-by Infektionen (Client seitige Schwachstellen)
- Download maliziöser Dateien
- (Office Dokumente, PDF, Executables)

Exponierte Dienste im Internet B



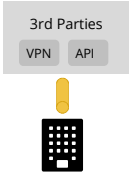
Gefährdungen
- Schwachstellen in externen Diensten (Software Bug, Fehlkonfigurationen) in Websites/Webserver/DB
- Schwachstellen oder missbrauch von Accounts in Remote Access Services (VPN, Citrix)

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

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

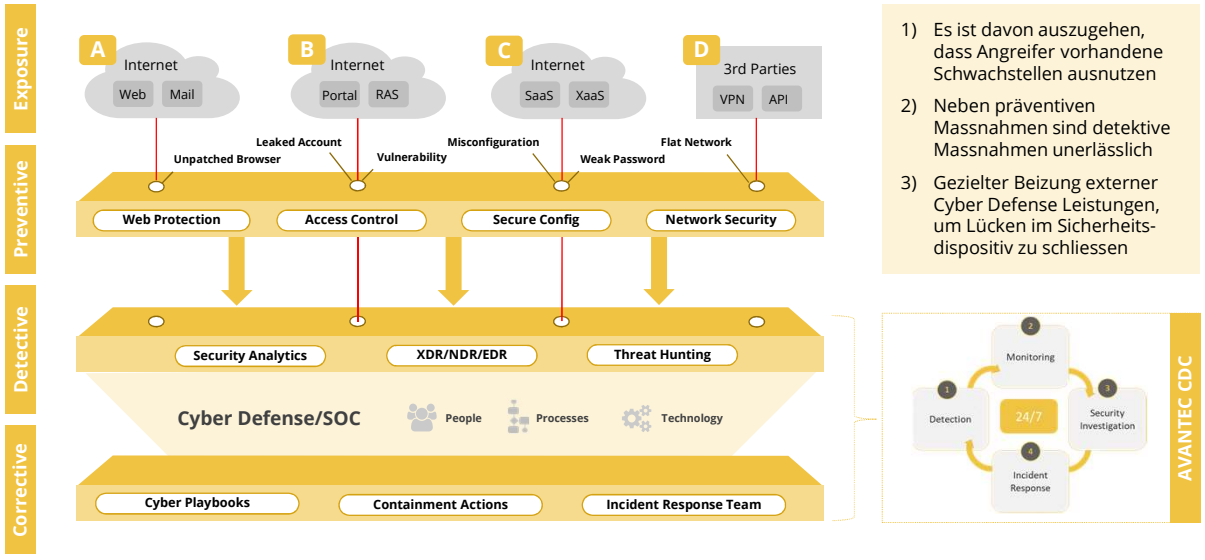
Herausforderungen

AVANTEC
Competence. Security. Trust.

- Professionellere Cyber Angriffe
- Steigende Komplexität
- Fehlendes Knowhow
- Mangelnde Awareness
- Diskrepanz Risiken & Sicherheitsbudgets
- Fehlende Ressourcen

Bewältigungsstrategie

AVANTEC
Competence. Security. Trust.



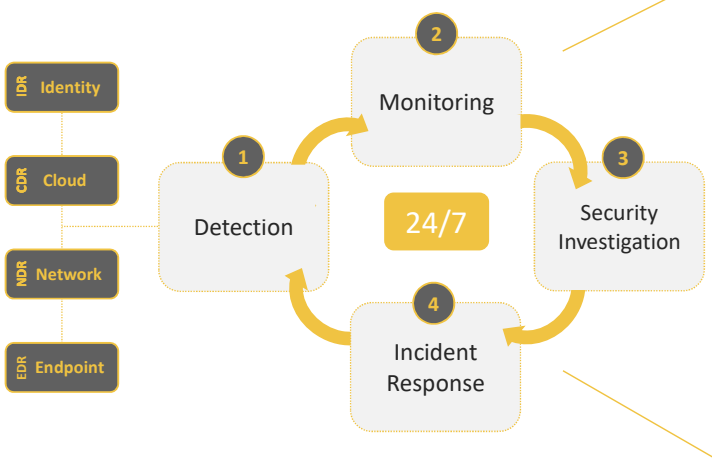
1) Es ist davon auszugehen, dass Angreifer vorhandene Schwachstellen ausnutzen
2) Neben präventiven Massnahmen sind detektive Massnahmen unerlässlich
3) Gezielter Beizung externer Cyber Defense Leistungen, um Lücken im Sicherheits-dispositiv zu schliessen

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

MDR Service

AVANTEC
Competence. Security. Trust.



Detection
Erkennung von abnormalem und maliziösem Verhalten mit State-of-the Art **Threat Detection 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

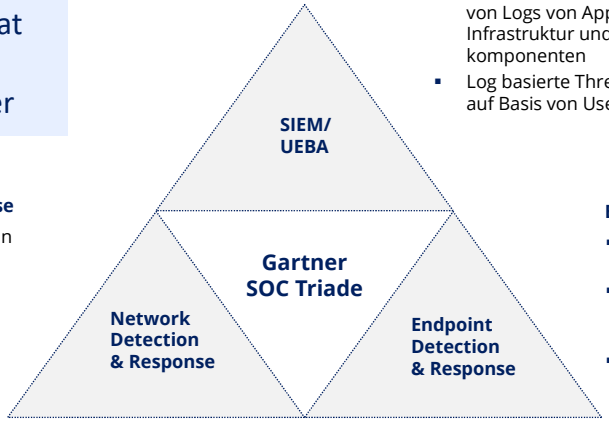
Threat Detection Komponenten

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 Sicherheits-komponenten
- 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
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

AVANTEC CDC / MDR Module

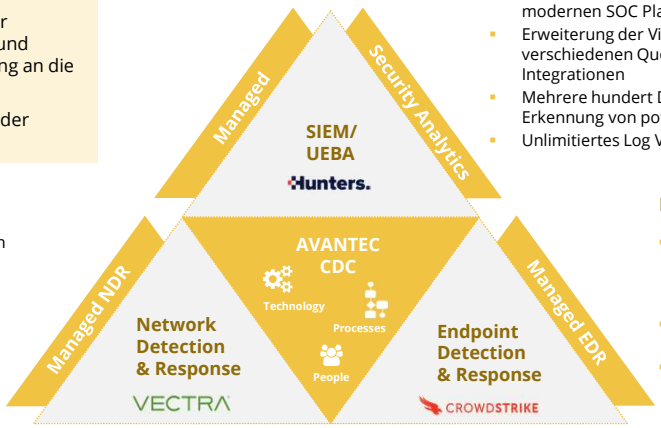
Modularer Aufbau der Services ermöglicht individuelle Zusammenstellung

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

Fazit

…und Empfehlungen aus unserer Erfahrung

1

Balance zwischen Prevention und Detection

- Fokus «historisch» eher auf Prevention – Detection (& Response) nach wie vor in vielen Unternehmen zu wenig ausgeprägt
- Zentralisierte Sicht (Korrelation) ermöglicht Cyber Angriffe überhaupt zu erkennen – und noch rechtzeitig mit Eindämmungsmassnahmen zu reagieren

2

Regelmässige Überprüfung der Sicherheitsmassnahmen

- Sicherheitsmassnahmen bedürfen einer regelmässigen Kontrolle bezüglich deren Effektivität (z.B. Coverage, Vulnerability Scanning, Security Review, Pentest, Config Review, internes Kontrollframework etc.)
- Gilt insbesondere auch für detektierende Massnahmen

3

Cyber Crisis Mgmt – im Ernstfall keine Zeit verlieren

- Eine gute Vorbereitung spart wertvolle Zeit, es empfiehlt sich klare Prozesse für die Bewältigung einer Cyber Krise zu definieren und diese regelmässige mit allen betroffenen zu trainieren – inkl. Senior Management

AVANTEC
Competence. Security. Trust.