IT-Sicherheitsgesetz 2.0 – Jetzt KRITIS-Anforderungen umsetzen!

Umgehend informiert sein, wenn ein Angreifer im Netzwerk ist!

Stellen Sie mit unserem Active Cyber Defense Service („ACD-KRITIS“) die Anomalie-Früherkennung sicher – 24/7!

ALLGEIER secion

Das IT-Sicherheitsgesetz 2.0 ist da! Setzen Sie jetzt mit unserem ACD-KRITIS Service die Gesetzesanforderungen innerhalb weniger Wochen um

Unternehmen aus dem Sektor der kritischen Infrastruktur (KRITIS) sind gemäß des IT-Sicherheitsgesetzes (IT-SiG) 2.0 u.a. dazu verpflichtet, Systeme zur Angriffsfrüherkennung zu implementieren. Gemeint ist hiermit ist ein aktiver Lösungsansatz, der nach verdächtigen Anomalien im eigenen Netzwerk sucht und Kompromittierungen umgehend aufdeckt und meldet. Mit Active Cyber Defense (ACD) erhält Ihre Organisation einen permanenten Managed Detection and Response Service, mit dem Sie - wie vom IT-SiG 2.0 g fordert – den kritischen Bereich in Ihrer IT-Sicherheit umgehend schließen.

ACD-KRITIS: Unser Service zur Angriffsfrüherkennung

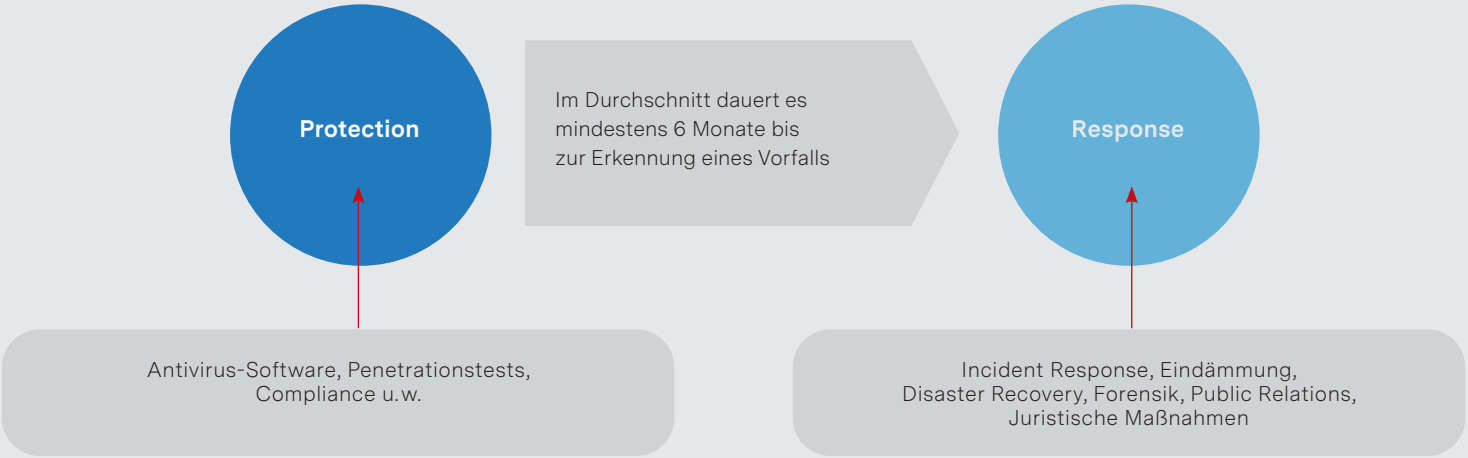
Unser 24/7 Incident Detection & Cyber Threat Hunting Service analysiert Ihr Netzwerk proaktiv und kontinuierlich auf Anomalien und identifiziert so die Kommunikation der Angreifer zu ihren Command & Control Servern (C&Cs).

Solche Attacken bleiben ohne entsprechende Detektierungsmaßnahmen i.d.R. lange Zeit unentdeckt: Im Schnitt dauert es sechs Monate, bis Unternehmen Angriffe dieser Art auf ihre Netzwerke identifizieren. Mit dem ACD-KRITIS Service stellen Sie sicher, dass Angreifer im eigenen Netz umgehend erkannt und entfernt werden, bevor Schaden entsteht. Im Falle einer detektierten Angriffsaktivität in Ihrem Netzwerk, die sofortigen Handlungsbedarf erfordert, werden Sie umgehend von unserem SOC-Team informiert und erreichen so eine Identifizierung von Sicherheitsvorfällen unmittelbar nach erfolgter Kompromittierung.

Mit ACD-KRITIS die Gesetzesanforderungen sofort umsetzen!

Gemäß IT-SiG 2.0 sind KRITIS Unternehmen verpflichtet, die Gesetzesanforderungen des IT-SiG 2.0 umzusetzen und Vorkehrungen zur proaktiven und umgehenden Abwehr von Cyberattacken zu treffen. Mit ACD-KRITIS erfüllen Sie gemeinsam mit uns diese Vorgaben in einem Bruchteil der Zeit: Die Implementierung unseres Active Cyber Defense Service dauert in der Regel max. 6 Wochen, abhängig von der Anzahl Ihrer Internetzugänge bzw. Unternehmensstandorte.

Zeitverlust im Protection- und Response-Prozess ohne Active Cyber Defense von Allgeier secion



Umgehende Identifizierung kompromittierter Systeme mit Active Cyber Defense von Allgeier secion

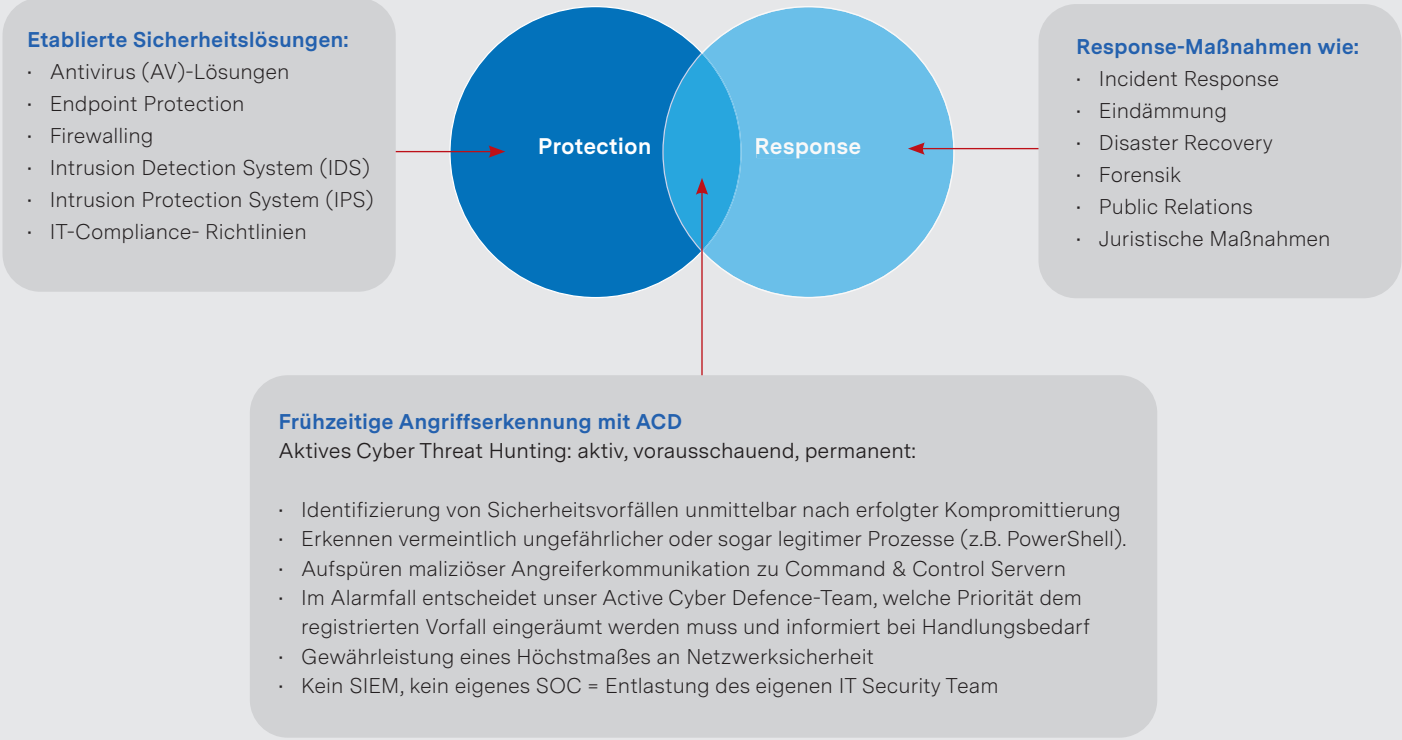


Abb 1: Schematischer Aufbau eines Protection- und Response-Prozesses ohne und mit Active Cyber Defense von Allgeier secion

Active Cyber Defense bildet das Bindeglied zwischen „Protection" und „Response". Es identifiziert frühzeitig mögliche Kompromittierungen und unterstützt somit den Protection- und Response-Prozess proaktiv und effektiv.

Mit Active Cyber Defense minimieren Sie die kritische Zeitspanne zwischen Versagen Ihrer Protection Tools und dem Einsatz Ihrer Response-Prozesse.

ACD-KRITIS

24/7 Netzwerksicherheit bei transparenten Kosten

- Profitieren Sie mit **ACD-KRITIS** von einem permanenten Managed Detection and Response Service zur frühzeitigen Angriffserkennung. Sie erreichen gemeinsam mit unserem ACD-KRITIS Team ein Höchstmaß an Transparenz über die Sicherheit und Integrität Ihres Netzwerkes.
- ACD-KRITIS ist als monatlicher Service buchbar und meldet 24/7 registrierte Verdachtsfälle in Ihrem Netzwerk. Unser ACD-KRITIS Team analysiert proaktiv Anomalien und zugrundeliegende Angriffsaktivitäten in Ihrem Netzwerk – und informiert Sie, sobald Handlungsbedarf erforderlich wird.
- Sie erreichen so eine Identifizierung von Sicherheitsvorfällen unmittelbar nach erfolgter Kompromittierung eines Systems – und nicht erst nach der riskanten durchschnittlichen Zeitspanne von 6 Monaten, in denen sich Angreifer unbeobachtet in Ihrem Netz bewegen, weiter ausbreiten und beliebig Daten ausleiten oder manipulieren.
- Mit ACD-KRITIS erfüllen Sie alle wesentlichen MUSS-Anforderungen für die drei Bereiche Protokollierung, Detektion und Reaktion (gemäß BSI Orientierungshilfe) und halten die geforderte Nachweispflicht ein.

Das unterscheidet ACD-KRITIS von anderen Incident Detection & Response-Lösungen!

- Unser ACD-KRITIS Service bezieht die **Überwachung aller Systeme Ihres Netzwerks** mit ein, wie beispielsweise Desktops, Laptops, Mobiltelefone, Tablets, Server, Netzwerk-Geräte, Drucker, IoT, ICS, BYOD.
- Für die Nutzung unserer ACD-KRITIS Lösung bedarf es **keiner Installation von Agents auf Clients** – es wird auf Netzwerkebene geprüft, ob Systeme zu Command & Control Servern kommunizieren und somit kompromittiert sind.
- Durch **Erkennen von auffälligem Kommunikationsverhalten** identifiziert ACD-KRITIS kompromittierte Systeme. Hierdurch können diese gezielt isoliert und zügig bereinigt werden.
- Wenn ein aktiv laufender Angriff identifiziert wird, stehen wir Ihnen bei Bedarf mit IR-Experten unmittelbar zur Seite. Unsere **IR-Prozesse sind speziell auf ACD-KRITIS abgestimmt:** Sie erhalten von uns direkt ein umfassendes Lagebild und wir begleiten Sie bei der Implementierung effektiver Gegenmaßnahmen.
- Unser **IR-Readiness Programm** ermöglicht Ihnen eine optimale Vorbereitung auf den Ernstfall: Neben proaktivem Austausch von Dokumenten und Definition von Notfallabläufen stellen wir Ihnen notwendige Werkzeuge und Härtungsempfehlungen bereit.

IT-SiG 2.0: Anomalie-Früherkennung fristgerecht sicherstellen!

Mit ACD-KRITIS gewährleisten Sie innerhalb weniger Wochen Ihre Network Security, unterstützt von einem effektiven System zur Angriffserkennung (SzA) – und das 24/7!

Entscheiden Sie sich für aktive Hacker-Jagd anstatt Post-Mortem-Forensik!

Mit ACD-KRITIS stellen Sie eine permanente proaktive Angriffsabwehr sicher, mit der Sie kostspielige reaktive Maßnahmen, wie beispielsweise aufwendige forensische Untersuchungen, vermeiden.

Post-Mortem-Forensik war gestern. Greifen Sie jetzt mit ACD-KRITIS an und jagen die Angreifer, bevor diese Schäden in Millionen-Höhe anrichten!

Sie planen den Aufbau eines SOC? Sparen Sie es sich!

Sie planen die Implementierung eines Security Operation Center (SOC) in Ihrem Unternehmen, aber verfügen nicht über das entsprechende Budget für ein angemessen großes Team? Mit unserem ACD-KRITIS Service decken Sie bereits die wichtigsten Anforderungen zu einer attraktiven monatlichen Servicepauschale ab!

Integrieren Sie mit ACD-KRITIS einen weiteren Security Layer – und optimieren Sie Ihre Ressourcen!

Sammeln Sie nicht mehr Unmengen an Logs – sparen Sie Unmengen an Zeit!

Log-Management und SIEM (Security Information and Event Management) haben das Ziel, Sicherheitsbedrohungen zu erkennen und jene unter Kontrolle zu halten, die ein maßgebliches Risiko für Ihre Organisation darstellen. Um diese zu identifizieren, müssen für ein Unternehmen jeden Tag Millionen Ereignisse ausgewertet werden – mit permanent aktualisierten Regelwerken.

Warum Terabytes an Logs sammeln, wenn Sie sich stattdessen auf die wirklich relevanten Informationen fokussieren können? Mit ACD-KRITIS gehört die zeitintensive Logfile-Analyse der Vergangenheit an!

Bereit für das IT-SiG 2.0?

Unsere Experten sind es auch! Nehmen Sie Kontakt zu uns auf:

Tel.: 040 38 90 71-0 E-Mail: info@secion.de

© Copyright 2023

Urheberrechtshinweis
Alle Inhalte dieses Dokuments, insbesondere Texte, Fotografien und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei der Allgeier secion, Zweigniederlassung der Allgeier CyRis GmbH.

Stand: August 2023

Allgeier secion,
Zweigniederlassung der Allgeier CyRis GmbH

Tel.: 040 389071-0
Fax: 040 389071-299
info@secion.de
www.secion.de

Paul-Dessau-Str. 8
22761 Hamburg