ALLGEIER
CyRis

Cyberangriffe frühzeitig erkennen und abwehren!

Angriffserkennung als Managed Service

– umfassend geschützt ohne eigene IT-Security-Abteilung

Unsere Cyber-Analysten überwachen mit modernsten Threat-Hunting-Methoden Ihr Netzwerk. Unsere 24/7-Überwachung gewährleistet, rechtzeitig auf etwaige Bedrohungen zu reagieren und geeignete Gegenmaßnahmen einzuleiten.

Cyberangriffe stellen eine dauerhaft hohe Bedrohung für die Geschäftstätigkeit und Compliance von Unternehmen dar. Ein eigenes Security Operations Center (SOC) ist aber für viele Firmen zu kosten- und zeitaufwändig. Daher nutzen immer mehr Unternehmen Services externer SOCs, die moderne Incident-Detection- und Threat-Hunting-Methoden nutzen.*

Nahezu wöchentlich wird von spektakulären Cyberangriffen berichtet, von denen immer wieder auch marktführende Unternehmen betroffen sind. Es ist offensichtlich, dass diese Angriffe trotz erheblicher IT-Security-Budgets und etablierter Sicherheitslösungen, wie Antivirus, Endpoint Protection, Firewalling und IDS/IPS, in zunehmendem Maße erfolgreich sind. Damit zeigt sich, dass diese etablierten Schutzmaßnahmen für aktuelle Bedrohungen nicht mehr ausreichend sind – und für Angreifer lediglich ein Ärgernis, jedoch kein tatsächliches Hindernis darstellen.

Unsere IT-Sicherheitsexperten sehen als Konsequenz einen bedeutenden Paradigmenwechsel in der IT-Security:

Der Bereich Prävention ist lediglich als Teilbereich einer IT-Sicherheitsstrategie zu sehen – ebenso muss zwingend der tatsächliche Eintritt einer erfolgreichen Kompromittierung einbezogen werden. Diese Kompromittierung gilt es frühzeitig zu erkennen, um weitere Schäden abzuwenden.

Wie lange dauert es, bis Sie Angreifer in Ihrem Netzwerk erkennen?

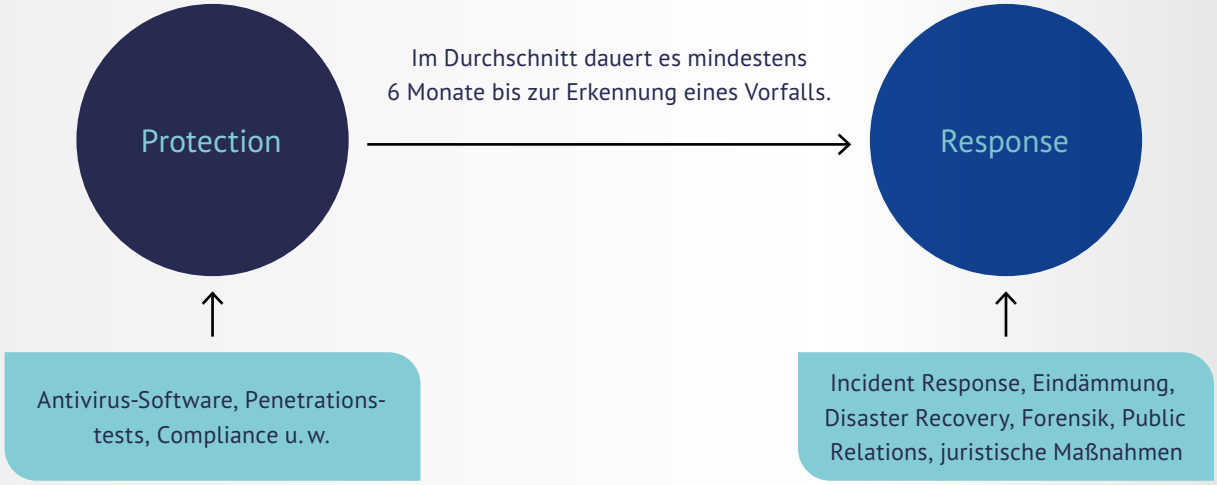
Derzeit vergehen noch immer durchschnittlich 6 Monate, bis eine Kompromittierung im Netzwerk identifiziert wird.

Mithilfe von Active Cyber Defense gewinnen Sie wertvolle Zeit!

Unser 24/7 Managed Detection and Response Service analysiert Ihr Netzwerk proaktiv und kontinuierlich im Hinblick auf Anomalien und identifiziert so die Kommunikation der Angreifer.

** Polaris Market Research Report, Security Operations Center (SOC) Forecast 2022–2030*

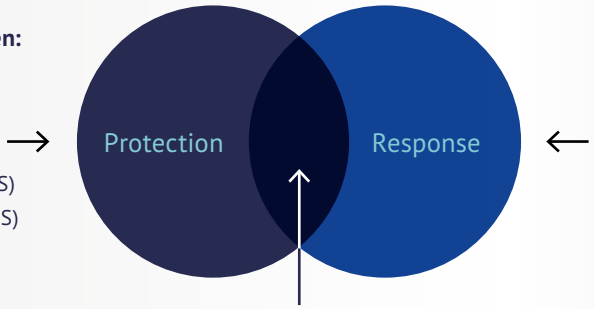
Zeitverlust im Protection- und Response-Prozess ohne Active Cyber Defense von Allgeier CyRis



Umgehende Identifizierung kompromittierter Systeme mit Active Cyber Defense von Allgeier CyRis

Etablierte Sicherheitslösungen:

- Antivirus (AV)-Lösungen
- Endpoint Protection
- Firewalling
- Intrusion Detection System (IDS)
- Intrusion Protection System (IPS)
- IT-Compliance-Richtlinien



Response-Maßnahmen wie:

- Incident Response
- Eindämmung
- Disaster Recovery
- Forensik
- Public Relations
- Juristische Maßnahmen

Frühzeitige Angriffserkennung mit ACD – Aktives Cyber Threat Hunting: aktiv, vorausschauend, permanent

- Identifizierung von Sicherheitsvorfällen unmittelbar nach erfolgter Kompromittierung
- Erkennen vermeintlich ungefährlicher oder sogar legitimer Prozesse (z. B. PowerShell).
- Aufspüren maliziöser Angreiferkommunikation
- Im Alarmfall entscheidet unser Active-Cyber-Defense-Team, welche Priorität dem registrierten Vorfall eingeräumt werden muss und informiert bei Handlungsbedarf
- Gewährleistung eines Höchstmaßes an Netzwerksicherheit

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

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.

Active-Cyber-Defense-Service

Investieren Sie in Ihre Netzwerksicherheit!

- Profitieren Sie mit Active Cyber Defense von einem permanenten Managed-Detection- and Response-Service. Sie erreichen gemeinsam mit unserem Active-Cyber-Defense-Team ein Höchstmaß an Transparenz über die Sicherheit und Integrität Ihres Netzwerkes.
- Active Cyber Defense ist als 24-monatiger Service buchbar und meldet 24/7 registrierte Verdachtsfälle in Ihrem Netzwerk an unsere Analysten. Unser Active-Cyber-Defense-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 und weiter ausbreiten.

Das unterscheidet Active Cyber Defense von anderen Incident-Detection- and Response-Lösungen!

- Unser Active-Cyber-Defense-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-Lösung bedarf es **keiner Installation von Agents auf Clients** – es wird auf Netzwerkebene geprüft, ob Systeme mit Command- & Control-Servern kommunizieren und somit kompromittiert sind.
- Durch **Erkennen von auffälligem Kommunikationsverhalten** identifiziert ACD-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. Unser **Incident-Readiness-as-a-Service ist speziell auf ACD abgestimmt**. Sie erhalten von uns direkt ein umfassendes Lagebild und wir begleiten Sie bei der Implementierung effektiver Gegenmaßnahmen.
- Unser **Incident-Readiness-as-a-Service** 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.

Investieren Sie noch immer Unsummen in Ihre IT-Security?

Mit unserem Active-Cyber-Defense-Service stellen Sie Ihre Network-Security sicher – und das 24/7!

Entscheiden Sie sich für eine aktive Hacker-Abwehr

Mit Active Cyber Defense stellen Sie eine permanente proaktive Angriffsabwehr sicher, mit der Sie kostspielige reaktive Maßnahmen, wie beispielsweise aufwendige forensische Untersuchungen, vermeiden.

Nutzen Sie Active Cyber Defense zu Ihrem Vorteil und vermeiden Sie somit Schäden in Millionenhöhe.

Sie planen den Aufbau eines SOCs? – Übergeben Sie dies lieber an unser Expertenteam.

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

Integrieren Sie mit Active Cyber Defense einen weiteren Security Layer – und optimieren Sie Ihre Ressourcen!

Verlassen Sie sich nicht mehr auf die zeitaufwendige Analyse von Logs.

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.

Wenden Sie sich an Ihren persönlichen Ansprechpartner unter:

0421 438 41 875 sales@allgeier-cyris.de

Impressum / V.i.S.d.P.

Herausgeber: Allgeier CyRis GmbH · Hans-Bredow-Straße 60 · 28307 Bremen
Redaktionsleitung: Sebastian Rüter · +49 40 389 071-172 · sebastian.rueter@allgeier-cyris.de
Grafikdesign: Tobias Wölky · www.woelky-grafik.de