TeamViewer

Bedrohungen proaktiv erkennen und Systeme umfassend schützen mit EDR

Maximilian Geiselhart

08.05.2024

Die Referenten

Maximilian Geiselhart

Sales Representative

Fabian Nordhus

Sr. Demand Gen Mgr. &
Deputy Team Lead Content
Marketing

Ablauf

1	ThreadDown Partnerschaft	5	Success Story
2	Neue Herausforderungen	6	Live-Demo
3	Ransomware	7	Q&A
4	Täter und Opfer		

ThreadDown Partnerschaft | 4 Gründe

1. ThreatDown gewinnt 10-mal in Folge die MRG Effitas Auszeichnung
2. 100% Erkennungsrate bei:
   - Online-Banking
   - Phishing
   - Ransomware
   - Exploits
3. Signatur- und verhaltensbasierte Erkennung
4. Rechenzentrum in Frankfurt

ThreatDown
Powered by Malwarebytes

Über 15 Jahre Erfahrung

Live Weltkarte

https://www.Malwarebytes.com/remediationmap

Herausforderungen | Früher

Standardverfahren:

- Firewall
- Backups
- Anti-Virus

Herausforderungen | Heute

Cybersecurity:
Erkennung von und Reaktion auf Bedrohungen
Einhaltung von Datenschutzgesetzen
Firewall- und Netzwerksicherheit
Endpunkt-Sicherheit
Sicherheitsschulung und Sensibilisierung
Planung der Reaktion auf Vorfälle

Infrastruktur-Management:
Netzwerküberwachung und -verwaltung
Server-Verwaltung
Speicherverwaltung
Virtualisierungstechnologien (z. B. VMware, Hyper-V)
Cloud-Infrastruktur (z. B. AWS, Azure, GCP)
Patch-Verwaltung
Sicherung und Wiederherstellung im Katastrophenfall

Monitoring:
Überwachung der Netzwerke
Anwendungsverwaltung
Überwachung der Kommunikations- und Kollaborationswerkzeuge:
E-Mail-Systeme (z. B. Microsoft Exchange, Google Workspace)
VoIP-Systeme
Werkzeuge für Videokonferenzen (z. B. Zoom, Microsoft Teams)

Mobilitäts- und Remotelösungen:
Virtuelle private Netzwerke (VPNs)
Verwaltung mobiler Geräte (MDM)
Remote-Desktop-Lösungen

Einhaltung von Vorschriften und Berichterstattung:
Compliance-Prüfung und -Berichterstattung
IT-Verwaltung
Risiko-Management

Technologiemanagement:
Bereitstellung und Verwaltung von Betriebssystemen (z. B. Windows, Linux)
Anwendungsmanagement (z. B. Microsoft 365, Salesforce)
Datenbankverwaltung (z. B. SQL Server, Oracle)
Middleware Management

Strategische IT Beratung:
IT-Budgetplannung
Technologie-Roadmapping
Planung der Geschäftskontinuität

Automatisierung and Optimierung:
Prozessautomatisierung
IT-Betriebsanalyse
Asset Management

Künstilich Intelligenz
Deep Fakes
IoT Bedrohungen
Supply Chain Angriffe

Ransomware

Großen Schaden anrichten
mit wenig Aufwand

- Finanziell äußerst lukrativ
- Breite Angriffsfläche
- Verheerende Auswirkungen
- Schwierig zu bekämpfen

Ransomware

Großen Schaden anrichten
mit wenig Aufwand

Kosten:

- Lösegeld von ⌀ 150.000 €*
- Betriebsausfälle (⌀ 23 Tage*)
  - Produktionsausfälle
  - Auftragsbearbeitung
  - Kundenlieferungen
  - Kommunikation
- Rufschädigung

*Quelle: Studie Branchenverband Bitkom 2022

Sind Sie die Zielscheibe? KMUs im Visier!

Kriminelle haben es auf leichte Ziele abgesehen

82%

der Ransomware-Angriffe richteten sich gegen Unternehmen mit weniger als 1.000 Mitarbeitern*

*Quelle: Studie Branchenverband Bitkom 2022

Success Story

- Eines der größten Lebensmittel- und Getränkeunternehmen weltweit
- Über 38.000 Mitarbeiter in über 40 Ländern

- Herausforderungen:
  - Schwierigkeiten bei der Identifizierung infizierter Endpunkte
  - Zeitaufwendige Endpunkt-Bereinigungsprozesse

- Lösung:
  - Automatisierte Sicherheitsprozesse
  - Integration mit bestehenden Sicherheitsinvestitionen

- Vorteile:
  - Beschleunigte Reaktionszeit auf Vorfälle auf Minuten reduziert
  - Risiko eines Datenverstoßes verringert
  - Vollautomatische Endpunkt-Bereinigung

Success Story

„ Die Endpunkt-Bereinigung von Malwarebytes ist von Anfang bis Ende vollständig automatisiert. Unser Sicherheitsteam muss nicht einmal eingreifen. Für uns ist es eine perfekte Lösung - es funktioniert einfach. „

Chris Leonard, Senior Manager bei Kraft Heinz

Live Demo

TeamViewer

Vielen Dank

Maximilian Geiselhart
Sales Representative
Maximilian.Geiselhart@TeamViewer.com
+49 7161 60692 50
Göppingen